

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

HEWLETT PACKARD ENTERPRISE
COMPANY,

Plaintiff,

v.

INTELLECTUAL VENTURES I LLC and
XENOGENIC DEVELOPMENT LIMITED
LIABILITY COMPANY,

Defendants.

Civil Action No. 22-cv-730-GBW-CJB

ANSWER AND COUNTERCLAIMS

Defendants answer the numbered paragraphs of the complaint:

1. Admitted that HPE is, *inter alia*, a global edge-to-cloud company. Otherwise denied.
2. Admitted.
3. Admitted, to the extent that IV is a corporation organized and existing under the laws of the state of Delaware with a registered agent located at 251 Little Falls Drive, Wilmington, DE 19808. Otherwise denied.
4. Admitted to the extent that Xenogenic is a corporation organized and existing under the laws of the state of Delaware with a registered agent located at 251 Little Falls Drive, Wilmington, DE 19808. Otherwise denied.
5. Admitted.
6. Admitted.
7. Denied.
8. Admitted.

9. Admitted as to the United States Patent and Trademark Office issuing United States Patent No. 7,246,173 (“the ’173 patent”) on July 17, 2007, entitled “Method and Apparatus for Classifying IP Data” to Franck Le and Haihong Zheng, and that a copy of the ’173 patent was attached to the Complaint as Exhibit 2. Otherwise denied.

10. Admitted as to the United States Patent and Trademark Office issuing United States Patent No. 7,505,751 (“the ’751 patent”) on March 17, 2009, entitled “Wireless Mesh Architecture” to Floyd Backes, and that a copy of the ’173 patent was attached to the Complaint as Exhibit 3. Otherwise denied.

11. Admitted.

12. Admitted.

13. Admitted.

14. Admitted that IV and HPE have spoken several times since 2021 regarding a potential license for HPE to IV’s patent portfolio, and that these communications have included discussions regarding certain patents. Otherwise denied.

15. Admitted.

16. Admitted.

17. Admitted.

18. Admitted.

19. Admitted that IV notified HPE of HPE’s infringement before filing the three identified lawsuits. Otherwise denied.

20. Admitted that IV sent the presentation attached as Exhibit 7 to the Complaint and that the DJ Patents are listed among more than 300 patents in the presentation. Otherwise denied.

21. Admitted that the slide states that the DJ patents are among 37 listed as “relevant to HPE” as to HPE’s Intelligent Edge in the Router / Wi-Fi Connectivity and Switching / Networking technology areas; that the HPE products at issue in HPE’s Complaint are within those technology areas identified by IV; and that three other patents among those 37 were asserted against certain Aruba products in the -226 case. Otherwise denied.

22. Admitted.

23. Admitted.

24. Admitted.

25. Admitted that the presentation included the described statements and that a telephone call took place between HPE and IV in March 2022. Otherwise denied.

26. Denied.

27. Defendants incorporate by reference their above responses.

28. Admitted.

29. Denied.

30. Denied.

31. Admitted.

32. Admitted.

33. Defendants incorporate by reference their above responses.

34. Admitted.

35. Defendants lack knowledge or information sufficient to form a belief about the truth of these allegations.

36. Defendants lack knowledge or information sufficient to form a belief about the truth of these allegations.

37. Denied.
38. Denied.
39. Defendants incorporate by reference their above responses.
40. Admitted.
41. Denied.
42. Denied.
43. Denied, insofar as Xenogenic is no longer the assignee of the '751 patent.
44. Admitted.
45. Defendants incorporate by reference their above responses.
46. Admitted.
47. Denied.
48. Denied.
49. Admitted.
50. Admitted.
51. Defendants incorporate by reference their above responses.
52. Admitted.
53. Denied.
54. Denied.
55. Admitted.
56. Admitted.

AFFIRMATIVE DEFENSES

1. HPE has failed to state a proper claim for relief.
2. HPE has failed to allege a sufficient case or controversy.

3. Effective July 27, 2022, IV assigned all rights, title and interests in the '173 patent to a third party, including the rights to sue for past, present and future damages. As such, defendants have no ability to assert the '173 patent against HPE, and there is no remaining case or controversy as to it between HPE and defendants.

4. Effective November 10, 2022, Xenogenic assigned all rights, title and interests in the '751 patent to Intellectual Ventures II LLC ("Intellectual Ventures II"), including the rights to sue for past, present and future damages. As such, there is no case or controversy as to the '751 patent between HPE and the named defendants.¹

5. Defendants reserve the right to assert additional claims and defenses.

COUNTERCLAIMS FOR PATENT INFRINGEMENT

Defendants, Intellectual Ventures II LLC ("Intellectual Ventures I") and Xenogenic Development Limited Liability Company ("Xenogenic"), for their counterclaims against plaintiff, Hewlett Packard Enterprise Company ("HPE"), alleges:

THE PARTIES

1. Intellectual Ventures I is a Delaware limited liability company having its principal place of business located at 3150 139th Avenue SE, Bellevue, Washington 98005.

2. Xenogenic is a Delaware limited liability company having its principal place of business located at 3150 139th Avenue SE, Bellevue, Washington 98005.

3. HPE is a corporation organized under the laws of Delaware.

¹ Counsel for the named defendants and Intellectual Ventures II notified counsel for HPE of the change in assignment on November 10, 2022, and informed HPE of their intention to file a motion to substitute Intellectual Ventures II as the assignee of the '751 patent. HPE did not respond to this request in time to file such a motion in conjunction with the instant Answer and Counterclaims. Defendants and Intellectual Ventures II intend to promptly file such a motion once the requirements of the Local Rules are met.

JURISDICTION

4. Defendants bring this action for patent infringement pursuant to 35 U.S.C. § 271, *et seq.* This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

FACTUAL BACKGROUND

5. Intellectual Ventures Management, LLC (“Intellectual Ventures”) was founded in 2000. Intellectual Ventures fosters inventions and facilitates the filing of patent applications for those inventions; collaborates with others to develop and patent inventions; and acquires and licenses patents from individual inventors, universities, corporations, and other institutions. A significant aspect of Intellectual Ventures’s business is managing the plaintiffs in this case, Intellectual Ventures I and Xenogenic.

6. One founder of Intellectual Ventures is Nathan Myhrvold, who worked at Microsoft from 1986 until 2000 in a variety of executive positions, culminating in his appointment as the company's first Chief Technology Officer in 1996. While at Microsoft, Dr. Myhrvold founded Microsoft Research in 1991 and was one of the world’s foremost software experts. Between 1986 and 2000, Microsoft became the world’s largest technology company.

7. Under Dr. Myhrvold’s leadership, Intellectual Ventures acquired thousands of patents covering many important inventions of the Internet era, including many pertaining to the wirelessly networked computers that comprise the Internet. Many of these inventions coincided with or shortly followed Dr. Myhrvold’s successful tenure at Microsoft.

8. HPE makes, uses, and sells 802.11 Wi-Fi access points (“APs”) in the United States, including the Aruba line of AP products.

9. Some of Aruba's APs implement the Device Provisioning Protocol ("DPP"), which is sometimes referred to as "Wi-Fi Easy Connect," including at least the 200, 300, 500 and 600 series APs.

10. Some of Aruba's APs implement Wireless Multimedia Extensions, or Wi-Fi Multimedia ("WMM").

11. Some Aruba APs implement tri-radio operation, including at least the Aruba 550 and 555 series running ArubaOS 8.6.0.0 and above.

12. Some Aruba APs implement 802.11ac beamforming.

THE PATENTS-IN-SUIT

13. On April 19, 2011, the United States Patent and Trademark Office ("USPTO") issued United States Patent No. 7,929,504 ("the '504 patent"), titled SYSTEMS AND METHODS FOR THE CONNECTION AND REMOTE CONFIGURATION OF WIRELESS CLIENTS, attached as Exhibit A.

14. The '504 patent is valid and enforceable.

15. Intellectual Ventures I is the owner and assignee of all rights, title, and interest in the '504 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

16. The '504 patent is directed to improved systems and methods of connection and remote configuration of wireless nodes communicating on a shared wireless communications channel. According to one embodiment, a wireless node may be remotely configured to connect to a communication network by configuring a master node to send it a frame with pre-configured configuration information for the wireless node. The frame with configuration information for the wireless node is sent across a wireless communication channel shared by both the master

node and the wireless node. The wireless communication channel may conform to the IEEE 802.11 standard, for example. The wireless node may receive and recognize the transmitted configuration frame. The wireless node may then configure itself according to configuration information in the received configuration frame, without requiring any inputting of configuration settings at the wireless node itself. The performance of wireless networks is thereby improved by the technologies disclosed and claimed in the '504 patent.

17. On March 23, 2010, the USPTO issued United States Patent No. 7,684,318 ("the '318 patent"), titled SHARED-COMMUNICATIONS CHANNEL UTILIZATION FOR APPLICATIONS HAVING DIFFERENT CLASS OF SERVICE REQUIREMENTS, attached as Exhibit B.

18. The '318 patent is valid and enforceable.

19. Intellectual Ventures I is the owner and assignee of all rights, title, and interest in the '318 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

20. The '318 patent claims and teaches improved methods for enabling latency-tolerant and/or latency intolerant applications running on wireless stations in a local area network, to intelligently share and use their shared-communications channel in a manner that seeks to satisfy quality-of-service the needs of the applications. According to one embodiment, the improved methods include queuing data frames to be transmitted during a transmitting station's transmit opportunity, wherein the data frames are queued in a queue, wherein the transmit opportunity corresponds to a length of time during which the transmitting station will transmit data frames from the queue to a shared-communications channel, and wherein the transmit opportunity is commenced with a control frame; and setting a length of time for the

transmit opportunity based on a priority of the queue. The performance of wireless networks is thereby improved by the technologies disclosed and claimed in the '318 patent.

21. On June 10, 2008, the USPTO issued United States Patent No. 7,386,036, titled WIRELESS MULTI-HOP SYSTEM WITH MACROSCOPIC MULTIPLEXING, attached as Exhibit C.

22. The '036 patent is valid and enforceable.

23. Intellectual Ventures I is the owner and assignee of all rights, title, and interest in the '036 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

24. The '036 patent is directed to an improved multi-hop wireless system (*e.g.*, a mesh network) in which radio links between relays and user equipment are optimized separately from the links between relays and base stations. According to one embodiment, the methods and systems include transceivers of at least three kinds with at least two kinds of radio interfaces. The first kind of transceiver, a base station (BS), is connected to the core network. The second kind of transceiver, a relay station (RS), is connected to the BS with a first radio interface, and to the third kind, the user equipment (UE), with a second radio interface. The first and second radio interfaces can operate, at least in part, using the same frequency bandwidth. Communication between relay station and the base station is processed separately from the communication between the user equipment and the base station. Among other advantages, the technologies disclosed and claimed in the '036 patent reduce complexity in scheduling transmissions over the wireless medium thereby increasing the performance of multi-hop wireless systems.

25. On November 26, 2013, the USPTO issued United States Patent No. 8,594,122 (“the ’122 patent”), titled CYCLIC DIVERSITY SYSTEMS AND METHODS, attached as Exhibit D.

26. The ’122 patent is valid and enforceable.

27. Intellectual Ventures I is the owner and assignee of all rights, title, and interest in the ’122 patent, including the rights to grant licenses, to exclude others, and to recover past damages for infringement.

28. The ’122 patent is directed to improved methods and systems for wireless network communication. According to one embodiment, a transmitter is configured to transmit a first communication frame from a first station to a second station; and provide a transmit announcement indication in the first communication frame, the transmit announcement indication indicating whether a second communication frame to the second station will follow the first communication frame. The indicated transmission does not need to include a MAC destination address because the transmission announcement indication was set on the preceding transmission to that station, thus reducing overhead. The performance of wireless networks is thereby improved by the technologies disclosed and claimed in the ’122 patent.

COUNTERCLAIM COUNT I

(HPE’s Infringement of U.S. Patent No. 7,929,504)

29. The preceding paragraphs are incorporated by reference.

30. The ’504 patent claims and teaches improved systems and methods for connections between and remote configurations of wireless nodes communicating on a shared wireless communications channel. According to one embodiment, a wireless node may be remotely configured to connect to a communication network by configuring a master node to

send it a frame with pre-configured configuration information for the wireless node. The frame with configuration information for the wireless node is sent across a wireless communication channel shared by both the master node and the wireless node. The wireless communication channel may conform to the IEEE 802.11 standard, for example. The wireless node may receive and recognize the transmitted configuration frame. The wireless node may then configure itself according to configuration information in the received configuration frame, without requiring any inputting of configuration settings at the wireless node itself.

31. As was known in the prior art, 802.11 wireless nodes may be configured locally at each wireless node such that they can connect to either an ad-hoc or infrastructure network. For example the wireless nodes may be supplied a BSSID, an encryption key, and a channel, which the wireless node uses to establish a connection. The wireless node is typically required to be physically present to input these configuration settings through a user interface. Additionally, some wireless nodes, such as cameras, phones, and printers, may not have a user interface at all, or the user interface may be difficult to use for entering the configuration information. Other methods of configuring wireless nodes may use a non-wireless connection, such as Ethernet or Universal Serial Bus (“USB”), however such configuration methods required additional hardware and circuitry that may not otherwise be necessary, and still required physical access to configure the wireless node.

32. In light of the above, the inventors of the ’504 patent recognized the need for improved systems and methods for connections between and remote configurations of wireless nodes communicating on a shared communications channel, which novel systems and methods are disclosed in the ’504 patent.

33. HPE has directly infringed and continues to directly infringe at least claim 1 of the '504 patent by making, using, selling, offering for sale, and importing products and services covered by that patent's claims. HPE's products and services that infringe the '504 patent include the Aruba line of access point ("AP") products with the Wi-Fi Easy Connect (a.k.a. Device Provisioning Protocol or DPP), including at least the 200, 300, 500 and 600 series APs; and all other Aruba APs or components incorporating Wi-Fi Easy Connect, made, used, sold, or offered for sale by or on behalf of HPE (collectively, "the '504 Accused Products").

34. Claim 1 of the '504 patent is reproduced below:

1. A method for remote configuration of a node comprising:
generating network configuration information at a first wireless node capable of
configuring a different second wireless node for network communications;
embedding a network identifier of a network for the second wireless node to join
within the network configuration information;
generating a frame having a destination address of the second wireless node and
including the network configuration information and an identifier to identify
the frame as a network configuration frame;
the first wireless node determining a channel that the second wireless node is
residing on; and
transmitting the frame from the first wireless node to the second wireless node on
the determined channel, the network configuration information designating
network configuration parameters to remotely configure the second wireless
node for the network communications.

35. The '504 Accused Products are configured to perform a method for remote configuration of a node by way of Wi-Fi Easy Connect. The Aruba 550 series AP is one example, seen below:

[HOME](#) / [PRODUCTS](#) / [WIRELESS](#) / [ACCESS POINTS](#) / [INDOOR ACCESS POINTS](#) / [ARUBA 550 SERIES](#)

Aruba 550 Series Indoor Access Points

Ultra-high-performing Wi-Fi 6 AP designed for environments such as large public venue locations, warehouse facilities, and extremely high-density locations.

[550 SERIES DATA SHEET →](#) [550 SERIES ORDERING GUIDE →](#)

CONTACT SALES

☆ Feedback



Minimum operating system software versions ^

ArubaOS and Aruba InstantOS 8.5.0.0

Source: <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/550-series/>

DEFINITION

WPA3

WPA3 vs WPA2

While WPA3 is more secure and comprehensive than WPA2, the WPA2 protocol will still be supported and updated by the Wi-Fi Alliance for the foreseeable future. When compared to the WPA2 standard, WPA3 adds the following notable features:

Simultaneous Authentication of Equals protocol: This is used to create a secure handshake, where a network device will connect to a wireless access point and both devices communicate to verify authentication and connection. Even if a user's password is weak, WPA3 provides a more secure handshake using Wi-Fi DPP.

Individualized data encryption: When logging on to a public network, WPA3 signs up a new device through a process other than a shared password. WPA3 uses a system called Wi-Fi Device Provisioning Protocol (DPP) which allows users to utilize [NFC](#) tags or [QR codes](#) to allow devices on the network. Further, WPA3 security uses GCMP-256 [encryption](#), compared to the previously used 128-bit encryption.

Source: <https://www.techtarget.com/searchsecurity/definition/WPA3>

WPA3: The Next Generation in Secure Mobility

By Dave Chen, Senior Product Marketing Manager

Share Post



04/2/18

Written by Dave Chen and Dan Harkins

The Wi-Fi Alliance has **recently announced** a new standard in wireless, **Wi-Fi CERTIFIED WPA3™**. WPA3 (Wi-Fi Protected Access) is designed as the successor to widely used WPA2 and brings a number of core enhancements to improve security protections and onboarding procedures across personal, public, and enterprise networks.

About the Author



Dave Chen

Senior Product Marketing Manager

Dave Chen is a Senior Product Marketing Manager at Aruba, a

Problem: Devices take time to onboard

Solution: DPP, or Device Provisioning Protocol, makes it easier to onboard headless devices, that may or may not have a touchscreen or keyboard with, say, a QR code.

Not strictly WPA3 per se, but DPP is marketed under the umbrella of WPA3. Imagine yourself with a brand new WeMo or Amazon Alexa. The typical procedure is to connect to the IoT device and manually enter the network SSID and password. As you connect more and more devices, especially in an enterprise setting where you may need to connect a plethora of Smart TVs, Apple HomePods, and connected lighting, scale becomes a huge problem.

DPP provisioning gives a certificate-like credential to these devices, and allows a trusted device to bootstrap another device onto a network with any of the following secure/unsecure methods:

- Scanning a QR code printed on the back
- Using a simple code or phrase
- Touching the device with NFC

Source: <https://blogs.arubanetworks.com/industries/wpa3-the-next-generation-in-secure-mobility/>

Aruba Enhanced Wi-Fi Security

WHAT IS WI-FI EASY CONNECT?

Wi-Fi Easy Connect is a new standard for secure device onboarding
It is based on Device Provisioning Protocol (DPP) and replaces WPS

DPP provides for simple and secure provisioning

- **Robust:** scanning a QR code is almost impossible to do wrong
- **Flexible:** mutual authentication or not depending on use case, no fixed roles, multiple bootstrapping techniques to allow for wide adoption
- **Secure:** even with non-mutual authentication there is still a level of trust—no leaps of faith required, no “soft-AP” provisioning necessary on Enrollee
- **Efficient:** elliptic curve cryptography provides strong keys with efficient operations that are sensitive to CPU-challenged devices

www.TechFieldDay.com
#MFD4

Source: : Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEA1AT3-sBM>)

Aruba Enhanced Wi-Fi Security

DPP WORKFLOW

- **Two players: a Configurator and an Enrollee (device to be configured)**
- **Configurator** defines network (SSID, access policy, etc)
- **Enrollees get configured**
 - Access Point is provisioned as “ap”
 - TV is provisioned as “sta”
 - Printer is provisioned as “sta”
 - DVR is provisioned as “sta”
- **Devices connect to DPP network on AP**
 - AP advertises a new AKM
 - Device exchanges connectors with AP, generates PMK
 - Device associates, 4-way handshake, secured connection

Additional devices are provisioned with just a point and click
Configurator not involved in the network after provisioning a device

www.TechFieldDay.com
#MFD4

Source: : Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEA1AT3-sBM>)

Aruba Enhanced Wi Fi Security

HOW IS ARUBA IMPLEMENTING DPP?

DPP

802.11 wired

“relays” IP network “controller”

- Aruba app running on handheld
 - Scans QR code of IoT device
 - Sends bootstrapping URI info to Controller
- DPP over wired
 - Controller acting as Configurator
 - Relays merely encaps/decaps frames to convert between 802.11 and TCP
 - Controller initiates DPP to device
 - Device is provisioned into role, given connector credential
- IoT device connects to network
 - Discovers AP advertising DPP network
 - Performs DPP Network Access protocol
 - Derives PMK/PMKID
 - Performs 4way handshake
 - Securely connected!

Source: : Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEAlAT3-sBM>)

Aruba Enhanced Wi Fi Security

DEMO

ZEBRA

- Aruba Configurator App
 - User logs in to account
 - Scans DPP QR code
 - Bootstrapping data uploaded
 - Controller provisioned
 - DPP initiated
- Provisioned device automatically joins DPP network

Source: : Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEAlAT3-sBM>)



DPP addresses this gap by leveraging WPA3 to enhance certificate handling and provide robust, secure, and scalable provisioning of IoT devices in any commercial, industrial, government, or consumer application. DPP also supports legacy WPA2 connections.

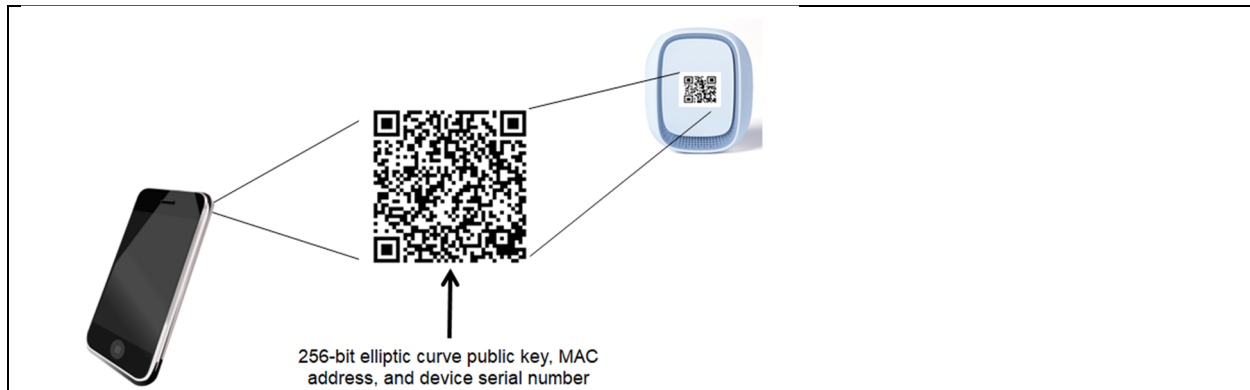


Figure 1. On-boarding Can Be As Simple As A QR Code

Designed to accommodate devices with or without a user interface, each DPP-enabled device is manufactured with an elliptic curve public/private key pair. The device can be brought onto a network via many paths, but the most common is by scanning a QR code on the device using a smartphone. The QR code contains an elliptic curve public key, and optionally the device's MAC address and serial number. Other bootstrapping methods are also available, including using near field communication (NFC) proximity to secure public key exchange and directly exchanging bootstrapping information with a cloud service.

Source: <https://www.arubanetworks.com/resource/securely-connect-iot-devices-to-in-building-it-networks>

Device Provisioning Protocol Specification v1.1



1 Introduction

This document is the technical specification for Wi-Fi CERTIFIED Easy Connect™, the Wi-Fi Alliance certification program for Device Provisioning Protocol (DPP). This specification defines the architecture, protocols, and functionality for Device Provisioning Protocol devices.

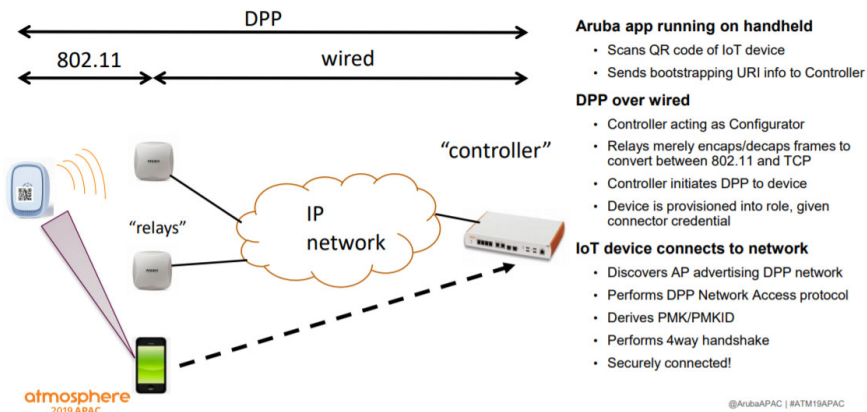
Source: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device_Provisioning_Protocol_Specification_v1.1_1.pdf (2018)

1 Introduction

This document is the specification for Wi-Fi CERTIFIED Easy Connect™, the Wi-Fi Alliance® certification program based on Wi-Fi Easy Connect™. This specification defines the architecture, protocols, and functionality for interoperability of Wi-Fi Easy Connect-certified devices. The terms "Device Provisioning Protocol" and "DPP" found throughout this document are interchangeable with "Wi-Fi Easy Connect".

Source: Source: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Easy_Connect_Specification_v2.0.pdf (2020)

How is Aruba Implementing DPP?



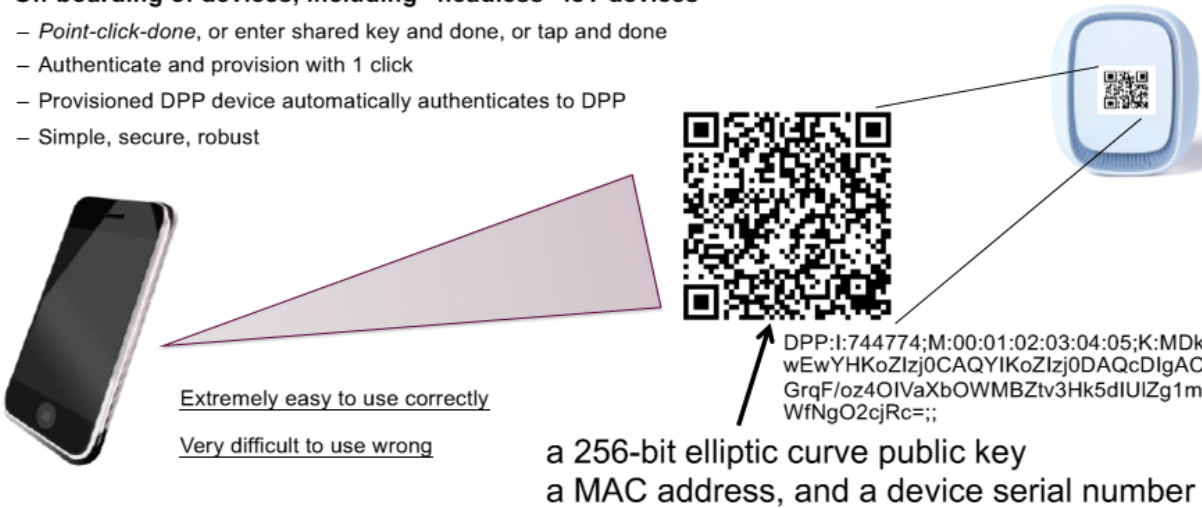
Source: <https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=f3d26a6d-4f36-473c-af86-d5aec13c9d74&forceDialog=0>



Source: https://www.clearToSend.net/wp-content/uploads/2019/10/MFD_August2019_Full_Deck_FINAL-copy.pdf

– **On-boarding of devices, including “headless” IoT devices**

- Point-click-done, or enter shared key and done, or tap and done
- Authenticate and provision with 1 click
- Provisioned DPP device automatically authenticates to DPP
- Simple, secure, robust



Extremely easy to use correctly
Very difficult to use wrong

DPP:I:744774;M:00:01:02:03:04:05;K:MDkwEwYHkoZlZj0CAQYIKoZlZj0DAQcDlGACGrqF/oz4OIvAXbOWMBZtv3Hk5dIUIG1mWfNgO2cjRc=;;

a 256-bit elliptic curve public key
a MAC address, and a device serial number

Source:
<https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=f3d26a6d-4f36-473c-af86-d5aec13c9d74&forceDialog=0>

How does DPP Work?

Two players– Initiator and Responder– in one of two roles– Configurator or Enrollee

Four phases in DPP: bootstrapping, authentication, provisioning, network connection

Bootstrapping– Gaining trust in the public key of an unknown and unauthenticated device

- Typically a CA does this but in DPP there is no CA
- Bind a device to its public key such that the public key becomes its identifier and the device proves who it is by using the corresponding private key

Authentication– Using the trusted, bootstrapped, key to ensure the right device is being spoken to

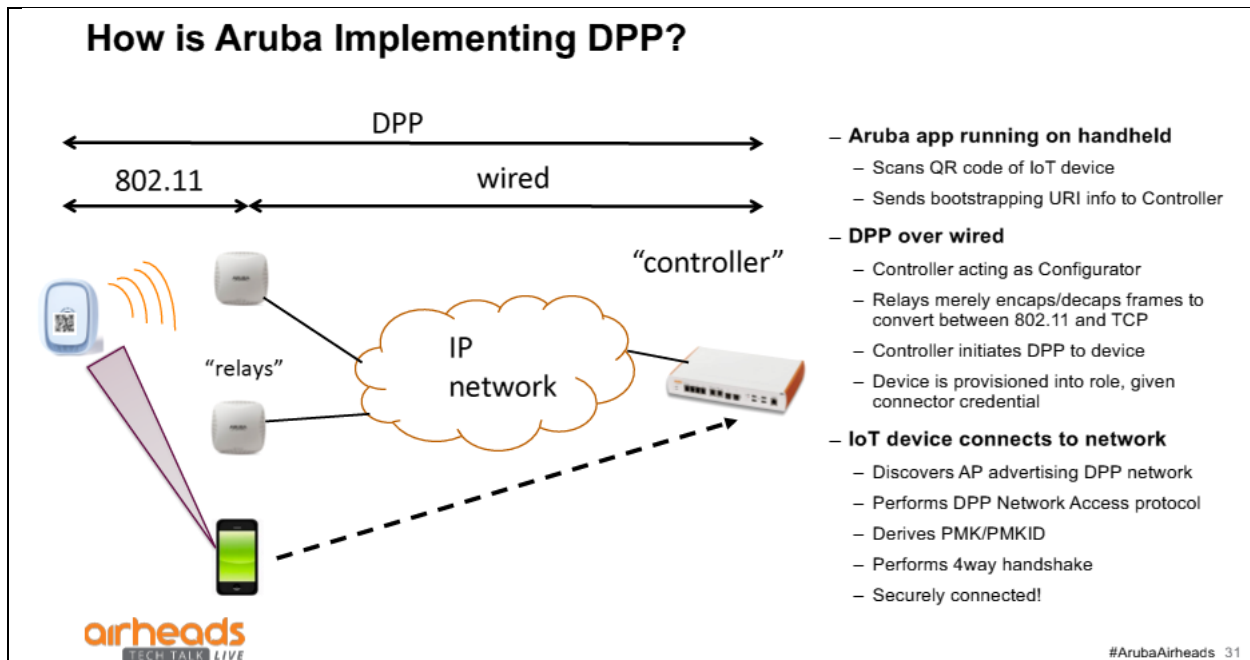
- Responder proves possession of private analog to bootstrapping public key
- Allows for mutual authentication and a form of non-mutual authentication that retains a degree of trust

Provisioning– Authenticated Enrollee requests provisioning, Configurator does provisioning

Network Access– A DPP-provisioned device communicates with another DPP-provisioned device

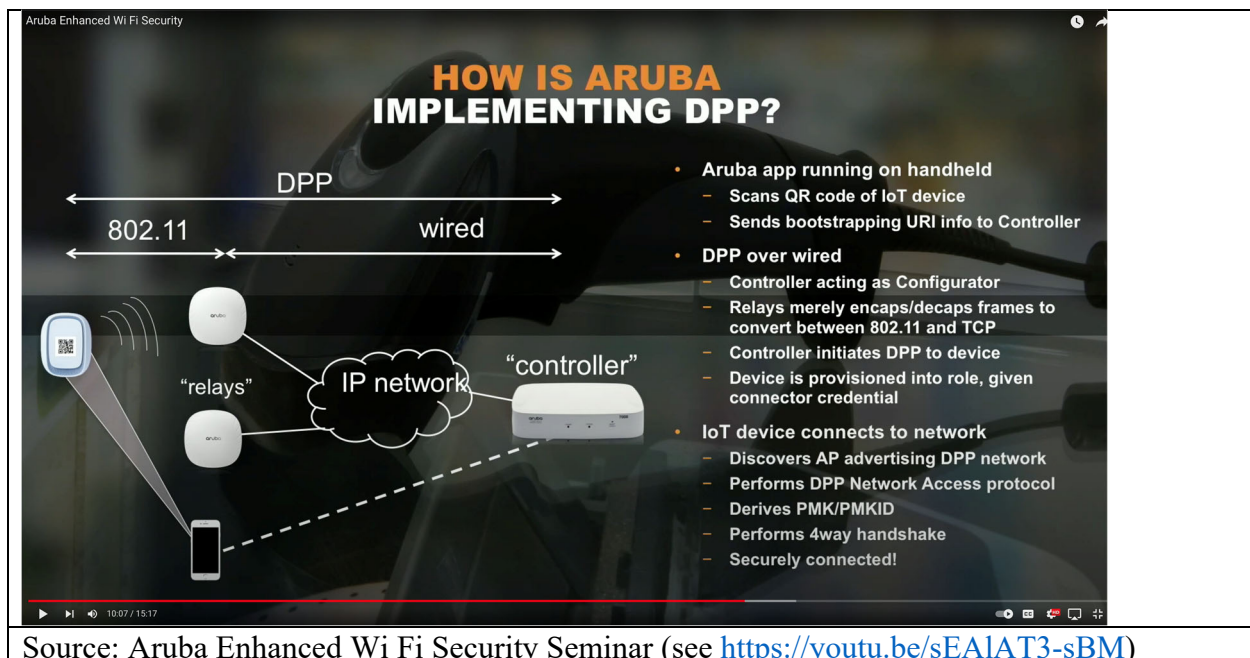
- Each device exchanges a *Connector*– a devices network access key signed by the Configurator
- Devices do a Diffie-Hellman with each other’s *Connectors* to derive a Pairwise Master Key (PMK)

Source:
<https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=cffaf7f5-c70c-4785-9342-0a9c8ac8d136>



Source:

<https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=cffaf7f5-c70c-4785-9342-0a9c8ac8d136>



Source: Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEA1AT3-sBM>)

36. The method practiced by the '504 Accused Products includes generating network configuration information at a first wireless node capable of configuring a different second wireless node for network communications:

Aruba Enhanced Wi Fi Security

HOW IS ARUBA IMPLEMENTING DPP?

The diagram illustrates the DPP implementation process. It shows an IoT device scanning a QR code, which is then processed by a handheld device. The IoT device connects to a network via relays and a controller. The diagram includes labels for 802.11, wired, and IP network connections.

- Aruba app running on handheld
 - Scans QR code of IoT device
 - Sends bootstrapping URI info to Controller
- DPP over wired
 - Controller acting as Configurator
 - Relays merely encaps/decaps frames to convert between 802.11 and TCP
 - Controller initiates DPP to device
 - Device is provisioned into role, given connector credential
- IoT device connects to network
 - Discovers AP advertising DPP network
 - Performs DPP Network Access protocol
 - Derives PMK/PMKID
 - Performs 4way handshake
 - Securely connected!

Source: Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEAlAT3-sBM>)

The STA Enrollee initiates the provisioning phase by transmitting a DPP Configuration Request frame, and is provisioned with configuration information in a DPP Configuration Response frame. After successfully receiving the DPP Configuration Response frame, the Enrollee is provisioned with the information required to establish secure access to the AP.

8.2.2.3 DPP Configuration Response frame

The DPP Configuration Response frame is transmitted by a DPP Configurator to a DPP Enrollee in response to DPP Configuration Request frame.

The DPP Configuration Response frame is a GAS Initial Response frame with vendor specific content and is constructed using the information in Table 33.

Table 34. Attributes in the DPP Configuration Response frame

Attribute	Required (R) / Optional (O) / Conditional (C)	Notes
DPP Status	R	Error code
Wrapped Data	R	Ciphertext output of AES-SIV wrapping of sub-attributes.
Enrollee Nonce	R	This attribute is a component of Wrapped Data
DPP Configuration object	C	The JSON encoded DPP Configuration object. This is a component of Wrapped Data. This attribute is only present when the DPP Status attribute contains STATUS_OK.

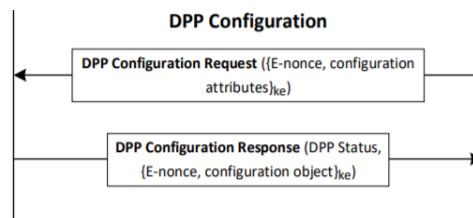


Figure 3. DPP message flow for DPP Provisioning of an STA Enrollee

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1

<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

4.3 DPP Configuration object

A Configurator provisions an Enrollee with information to discover a network as well as credentials to establish secure access to the network.

The DPP Configuration object contains the following nodes:

- Wi-Fi Technology: the Wi-Fi technology that is being provisioned
- DPP Discovery: Information provided for network/device discovery
- DPP Credential: Credential information for network access

4.3.1 Wi-Fi Technology

The Wi-Fi Technology node identifies the Wi-Fi technology of the policy that is to be provisioned within the Enrollee device. It may have one of the following values:

- DPP Configurator, if the enrollee is provisioned as a Configurator
- Infrastructure, if the enrollee is provisioned as either a STA or an AP
- Peer to Peer (P2P)², if the enrollee is provisioned as a P2P Device

The Configurator shall set the value of this node depending on the Wi-Fi Technology that is in operation between the Enrollee and the Configurator.

The Enrollee reads the value of this node to determine the type of provisioning system to use.

4.3.2 DPP Discovery

The DPP Discovery node contains optional operating/discovery information such as SSID, operating channel and operating band.

The Configurator sets the value of this node to the values of a Wi-Fi network (for example SSID and channel) that are to be provisioned within the client device.

The Enrollee reads the value of this node and provisions the Wi-Fi network information.

4.3.3 DPP Credential

The DPP Credential node contains the credential information provisioned in the Enrollee to obtain secure network access.

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

37. The method practiced by the '504 Accused Products includes embedding a network identifier of a network for the second wireless node to join within the network configuration information:

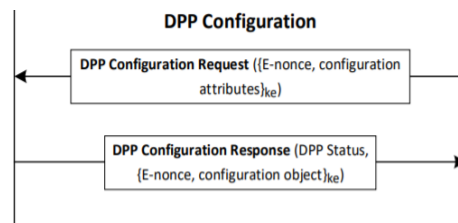


Figure 3. DPP message flow for DPP Provisioning of an STA Enrollee

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

The encoded configuration information includes a configuration object which contains the configuration objects below:

- A Wi-Fi technology object which specifies the type of connection, such as an AP infrastructure connection
- A discovery object which includes the service set identifier (SSID)
- A credential object which includes the security credential information

Source: <https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi%20CERTIFIED%20Easy%20Connect%20Technology%20Overview.pdf>

Otherwise, the Configurator uses the attributes supplied by the Enrollee to construct a confirmation message consisting of a DPP Configuration object (see section 6.3.6) and the received E-nonce. This message is wrapped with ke . The ciphertext output by AES-SIV is then, together with a DPP Status field set to STATUS_OK, copied into a DPP Configuration Response frame and sent to the Enrollee.

Configurator → Enrollee: DPP Status, { E-nonce, configurationObject }_{ke}

Table 14. DPP Configuration object parameters

Parameter	Name	Type	Value	Description
DPP Configuration object	configurationObject	OBJECT		
Wi-Fi Technology object:	wi-fi_tech	STRING	infra	Future revisions may include the values dpp_config, nan, p2p, asp2.
Service	svc	STRING		Optional parameter depending on the value of wi-fi_tech
Discovery object:	discovery	OBJECT		
SSID	ssid	STRING	alpha numeric	The name of the network to connect to

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

38. The method practiced by the '504 Accused Products includes generating a frame having a destination address of the second wireless node:

Aruba Enhanced Wi Fi Security

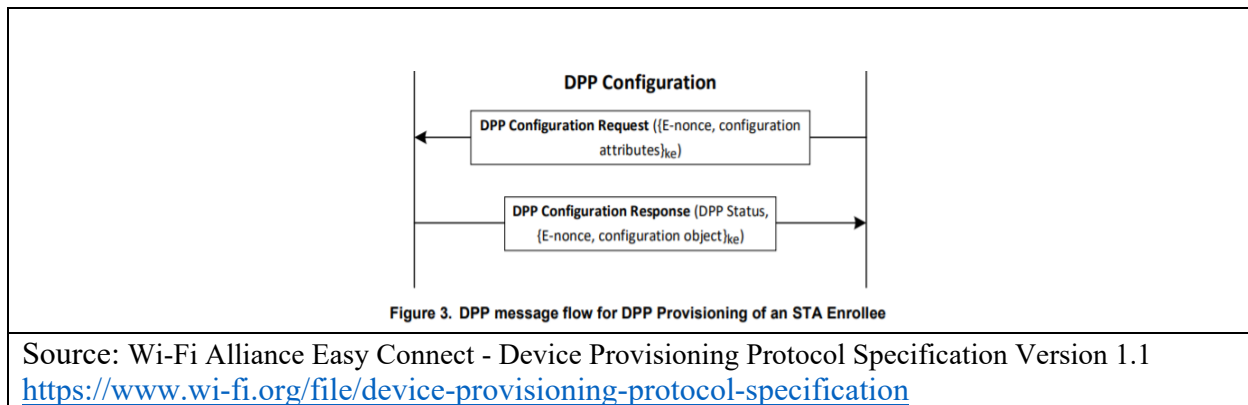
HOW IS ARUBA IMPLEMENTING DPP?

The diagram illustrates the DPP implementation process. It shows a handheld device (IoT device) scanning a QR code and sending bootstrapping URI info to a controller. The controller acts as a configurator, relaying frames between the device and the network. The device connects to the network, discovers the AP, performs a 4-way handshake, and is securely connected. The diagram also shows the flow of DPP over 802.11 and wired networks, with relays and an IP network involved.

- Aruba app running on handheld
 - Scans QR code of IoT device
 - Sends bootstrapping URI info to Controller
- DPP over wired
 - Controller acting as Configurator
 - Relays merely encaps/decaps frames to convert between 802.11 and TCP
 - Controller initiates DPP to device
 - Device is provisioned into role, given connector credential
- IoT device connects to network
 - Discovers AP advertising DPP network
 - Performs DPP Network Access protocol
 - Derives PMK/PMKID
 - Performs 4way handshake
 - Securely connected!

Source: Aruba Enhanced Wi Fi Security Seminar (see <https://youtu.be/sEAlAT3-sBM>)

39. The method practiced by the '504 Accused Products includes generating a frame including the network configuration information:



The encoded configuration information includes a configuration object which contains the configuration objects below:

- A Wi-Fi technology object which specifies the type of connection, such as an AP infrastructure connection
- A discovery object which includes the service set identifier (SSID)
- A credential object which includes the security credential information

Source: <https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi%20CERTIFIED%20Easy%20Connect%20Technology%20Overview.pdf>

4.3.1 Wi-Fi Technology

The Wi-Fi Technology node identifies the Wi-Fi technology of the policy that is to be provisioned within the Enrollee device. It may have one of the following values:

- DPP Configurator, if the enrollee is provisioned as a Configurator
- Infrastructure, if the enrollee is provisioned as either a STA or an AP
- Peer to Peer (P2P)², if the enrollee is provisioned as a P2P Device

4.3.3 DPP Credential

The DPP Credential node contains the credential information provisioned in the Enrollee to obtain secure network access.

The credential information included in the configuration is dependent on the value of the AKM parameter. The AKM parameter may either be set to "dpp" to indicate that a Connector is being provisioned or "psk" if a legacy passphrase or pre-shared key is being provisioned. The DPP Credential may contain a Connector, C-sign-key, legacy PSK or passphrase.

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

40. The method practiced by the '504 Accused Products includes generating a frame including an identifier to identify the frame as a network configuration frame:

8.2.2.3 DPP Configuration Response frame

The DPP Configuration Response frame is transmitted by a DPP Configurator to a DPP Enrollee in response to DPP Configuration Request frame.

The DPP Configuration Response frame is a GAS Initial Response frame with vendor specific content and is constructed using the information in Table 33.

Table 33. General format of DPP Configuration Response frame

Field	Size (octets)	Value (Hexadecimal)	Description
Category	1	0x04	IEEE 802.11 Public Action frame usage. See Table 9-47 [2]
Action field	1	0x0B	IEEE 802.11 GAS Initial Response frame usage. See Table 9-307 [2]

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

9.6.8.1 Public Action frames

Table 9-307—Public Action field values

Public Action field value	Description
11	GAS Initial Response (see 9.6.8.13)

Source: IEEE Std 802.11-2016

- IEEE802.11u defines a protocol allowing to query additional information about the Wi-Fi access before initiating the association and authentication
- **GAS** (Generic Advertisement Service) provides a container for the ANQP (Access Network Query Protocol), which provides more information about the Wi-Fi access

Source: <https://www.ieee802.org/1/files/public/docs2013/new-maxriegel-enhanced-network-detection-0813-v01.pdf>

41. The method practiced by the '504 Accused Products includes the first wireless node determining a channel that the second wireless node is residing on:

4.3 DPP Configuration object

A Configurator provisions an Enrollee with information to discover a network as well as credentials to establish secure access to the network.

The DPP Configuration object contains the following nodes:

- Wi-Fi Technology: the Wi-Fi technology that is being provisioned
- DPP Discovery: Information provided for network/device discovery
- DPP Credential: Credential information for network access

4.3.2 DPP Discovery

The DPP Discovery node contains optional operating/discovery information such as SSID, operating channel and operating band.

The Configurator sets the value of this node to the values of a Wi-Fi network (for example SSID and channel) that are to be provisioned within the client device.

The Enrollee reads the value of this node and provisions the Wi-Fi network information.

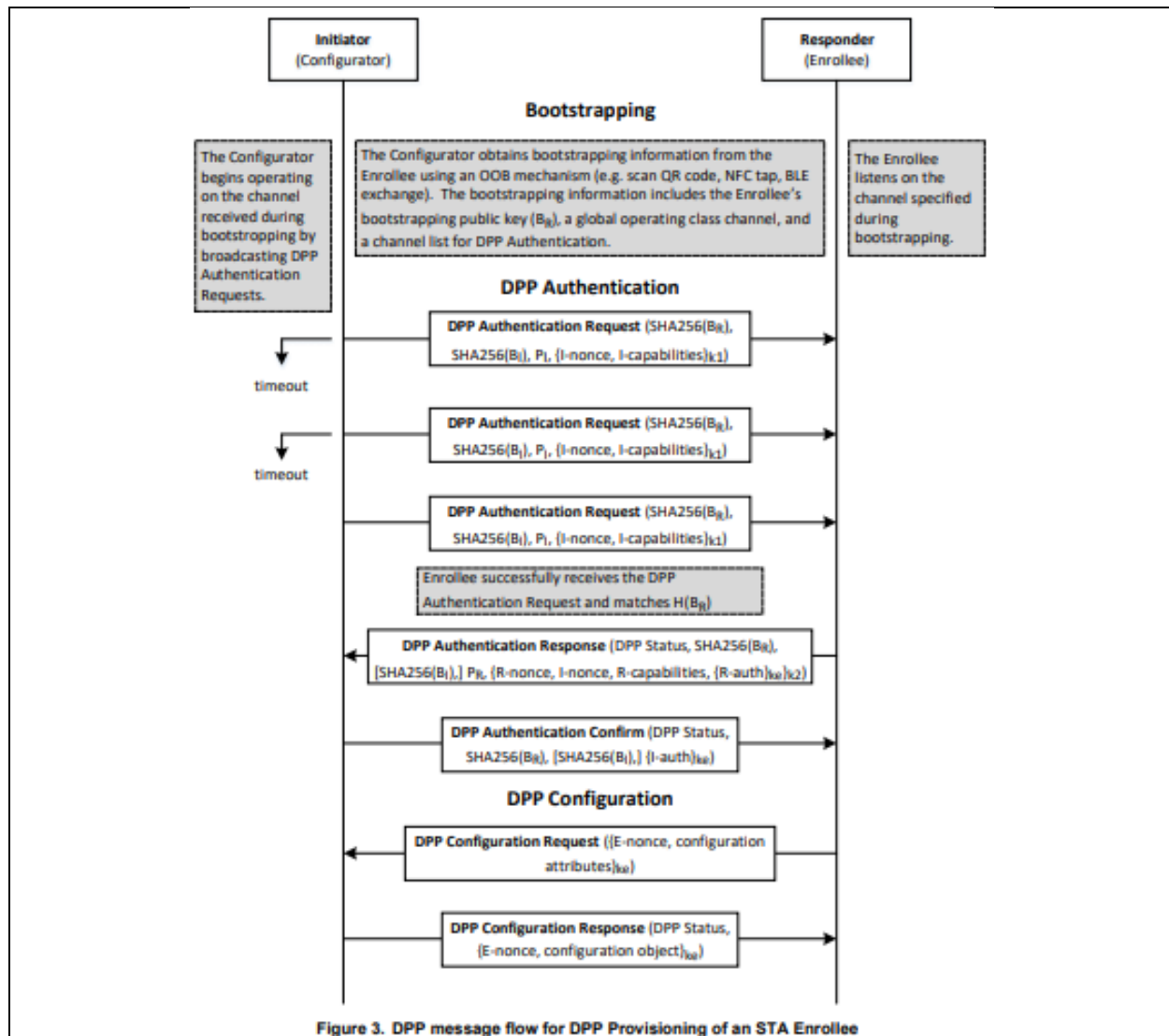
The DPP Configuration protocol exchange shall immediately follow a successfully completed DPP Authentication protocol exchange with the Enrollee sending the DPP Configuration Request within one second of the completion of DPP Authentication. Both the Enrollee and the Configurator shall use the same MAC addresses and the same channel that was used during DPP Authentication protocol exchange.

If the global operating class/channel list is included in the bootstrapping information, the device indicates that it shall be listening on one of the listed channels for other devices to initiate the DPP Authentication exchange. If this list is not included, the device does not provide any guidance on which channel it is listening on and the Initiator shall iterate over all available channels. Iteration over a large number of channels adds significant extra delay in the DPP Authentication exchange; therefore, devices using QR Code bootstrapping are recommended to include a single channel or at most a short list of possible channels in the bootstrapping information.

The Responder listens on channels included in the channel list provided in the bootstrapping information or on any available channel if the optional channel list is not provided, waiting to receive a DPP Authentication Request frame. Upon successful receipt of a DPP Authentication Request frame, the Responder transmits a DPP Authentication Response frame to the Initiator.

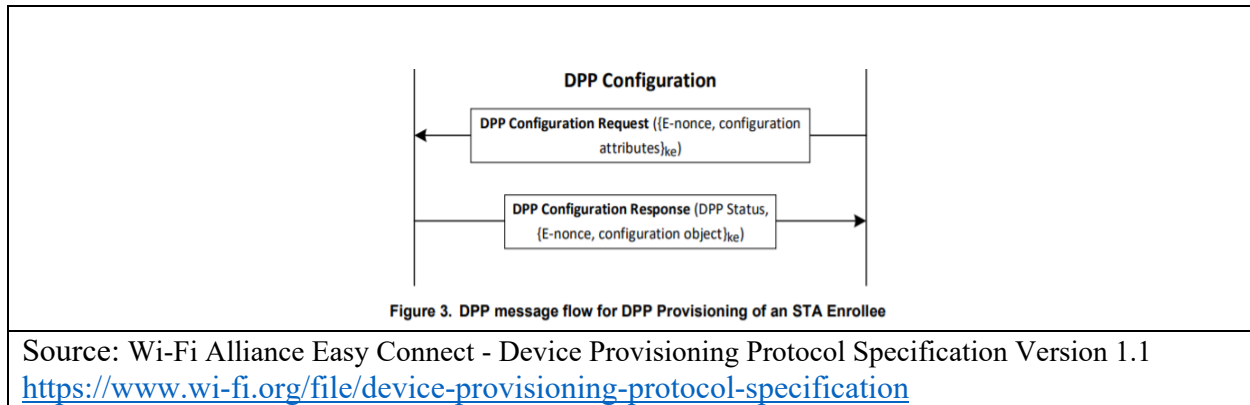
The Initiator shall determine the list of possible DPP authentication channels by taking the intersection of the channels it supports under the current regulatory requirements and the channels that are present in the bootstrapping information, if included. If the bootstrapping information does not include the optional channel list, the Initiator uses all the channels it supports under the current regulatory requirements as the list of possible DPP authentication channels. If the list of possible DPP authentication channels is empty, DPP authentication cannot be performed and the Initiator should notify the user.

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>



Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1
<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

42. The method practiced by the '504 Accused Products includes transmitting the frame from the first wireless node to the second wireless node on the determined channel, the network configuration information designating network configuration parameters to remotely configure the second wireless node for the network communications:



Once DPP Authentication is complete, the peer acting as the enrollee transmits a DPP Configuration Request frame to the Configurator.

Upon successful receipt of the DPP Configuration Request frame, the Configurator transmits the DPP Configuration Response frame to complete provisioning of the Enrollee.

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1

<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

The DPP Configuration protocol exchange shall immediately follow a successfully completed DPP Authentication protocol exchange with the Enrollee sending the DPP Configuration Request within one second of the completion of DPP Authentication. Both the Enrollee and the Configurator shall use the same MAC addresses and the same channel that was used during DPP Authentication protocol exchange.

Source: Wi-Fi Alliance Easy Connect - Device Provisioning Protocol Specification Version 1.1

<https://www.wi-fi.org/file/device-provisioning-protocol-specification>

43. HPE has had knowledge of the '504 patent since at least as early as the receipt of IV's presentation in April of 2022 presentation, which flagged the '504 patent; received further knowledge from IV's notice letter on November 13, 2022; and will receive further knowledge by service upon HPE of the Complaint in this Case.

44. Additionally, HPE has been, and currently is, an active inducer of infringement of the '504 patent under 35 U.S.C. § 271(b) and a contributory infringer of the '504 patent under 35 U.S.C. § 271(c).

45. HPE has actively induced, and continues to actively induce, infringement of the '504 patent by causing others to use, offer for sale, or sell products or services covered by the '504 patent, including the '504 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end-users, who, in turn, use, provision for use,

offer for sale, or sell those products and services, which directly infringe the '504 patent. HPE's inducement includes the directions and instructions found at:

- <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/550-series/>
- <https://blogs.arubanetworks.com/industries/wpa3-the-next-generation-in-secure-mobility/>
- <https://www.arubanetworks.com/resource/securely-connect-iot-devices-to-in-building-it-networks>
- <https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=f3d26a6d-4f36-473c-af86-d5aec13c9d74&forceDialog=0>
- <https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=cffaf7f5-c70c-4785-9342-0a9c8ac8d136>
- https://www.arubanetworks.com/assets/tg/TB_Aruba-Instant-Mode.pdf

46. HPE has contributed to, and continues to contribute to, the infringement of the '504 patent by others by selling the '504 Accused Products, which, when installed, configured, and used directly infringe the '504 patent.

47. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe, and would actively induce and contribute to the infringement of, the '504 patent.

48. HPE has committed, and continues to commit, contributory infringement by selling products and services that directly infringe the '504 patent when used by a third party, such as the '504 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the '504 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

49. As a result of HPE's acts of infringement, Intellectual Ventures I has suffered and will continue to suffer damages in an amount to be determined at trial.

COUNTERCLAIM COUNT II

(HPE's Infringement of U.S. Patent No. 7,684,318)

50. The preceding paragraphs are incorporated by reference.

51. The '318 patent claims and teaches improved methods for enabling latency-tolerant and/or latency intolerant applications running on wireless stations in a local area network, to intelligently share and use their shared-communications channel in a manner that seeks to satisfy the quality-of-service needs of the applications. According to one embodiment, the improved methods include queuing data frames to be transmitted during a transmitting station's transmit opportunity, wherein the data frames are queued in a queue, wherein the transmit opportunity corresponds to a length of time during which the transmitting station will transmit data frames from the queue to a shared-communications channel, and wherein the transmit opportunity is commenced with a control frame; and setting a length of time for the transmit opportunity based on a priority of the queue.

52. As was known in the prior art, many types of applications (*e.g.*, e-mail, ftp, http, voice, video, etc.) could send data across a local area network. The data for some of these applications—e-mail and web browsing for example—can be sent with a lesser degree of urgency. These types of applications are called “latency-tolerant.” In contrast, the data for some other applications—particularly those that comprise a real-time component like video and audio—must traverse the network with a greater degree of urgency. These applications are called “latency-intolerant.”

53. IEEE 802.11 local area networks were initially designed for latency-tolerant applications and typically each of those applications shared access to the shared-communications channel on an equal basis. This is usually acceptable for latency-tolerant applications. In

contrast, this is often unacceptable for latency-intolerant applications because giving equal access to latency-tolerant and latency-intolerant applications might prevent the latency-intolerant application from sending and receiving its data in a timely manner.

54. In light of the above, the inventors of the '318 patent recognized that if the latency-intolerant applications are deemed to be important, then a mechanism had to be introduced into the network so that the latency-intolerant applications could be given the amount of resources they needed in a timely manner. Therefore, the inventors of the '318 patent recognized the need for a technique for enabling latency-tolerant and latency-intolerant applications to intelligently share access to the shared-communication channel.

55. HPE has directly infringed and continues to directly infringe at least claim 1 of the '318 patent by making, using, selling, offering for sale, and importing products and services covered by that patent's claims. HPE's products and services that infringe the '318 patent include the line of access points (AP) with Wireless Multimedia Extensions, or Wi-Fi Multimedia ("WMM"), such as the Aruba AP-535; and all other Aruba access point products or components which include WMM operability made, used, sold, or offered for sale by or on behalf of HPE (collectively, "the '318 Accused Products").


56. Claim 1 of the '318 patent is reproduced below:

1. A method, comprising:

queuing data frames to be transmitted during a transmitting station's transmit opportunity, wherein the data frames are queued in a queue, wherein the transmit opportunity corresponds to a length of time during which the transmitting station will transmit data frames from the queue to a shared-communications channel, and wherein the transmit opportunity is commenced with a control frame; and

setting a length of time for the transmit opportunity based on a priority of the queue.

57. The '318 Accused Products are confirmed to perform a method for queuing data frames to be transmitted during a transmitting station's transmit opportunity. The Aruba 535 series AP, which implements WMM, is one example, as seen below:



The worldwide network of companies that brings you Wi-Fi®

Certified products, news, etc.

SEARCH

View Wi-Fi CERTIFIED™ products by category

Download your results

SHOW NAVIGATION

Product Finder

Filtered Results

Clear all filters

Keyword Search

ADD

Brand

X

Hewlett Packard Enterprise

Hide Advanced Filters

All Capabilities

Connectivity

Optimization

☐ TDLS

☐ Wi-Fi Data Elements™


☐ Wi-Fi Agile Multiband™

☐ ANQP


☐ Stream Classification Service

☒ WMM®


☐ Max Throughput




Product Name: AP-518
Model Number: AP518
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2022-11-03




Product Name: AP-505H
Model Number: AP505H
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2022-11-03



Product Name: AP565
Model Number: AP565
Total Variants: 1 (1 result)



Product Name: AP-503
Model Number: AP-503
Total Variants: 1 (1 result)



Product Name: Aruba Multiservice Mobili...
Model Number: AP-535
Total Variants: 5 (5 results)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2022-06-01

Source: https://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&certifications=586&companies=301

ARUBA 530 SERIES WIRELESS ACCESS POINTS

Very high Wi-Fi 6 (802.11ax) performance with dual radios



Certifications

- Wi-Fi Alliance:
 - Wi-Fi CERTIFIED a, b, g, n, ac
 - Wi-Fi CERTIFIED 6 (ax)
 - WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE)
 - WMM, WMM-PS, Wi-Fi Vantage, Wi-Fi Agile Multiband

Regulatory model numbers

- AP-534: APIN0534
- AP-535: APIN0535

Source: https://www.arubanetworks.com/assets/ds/DS_AP530Series.pdf

Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED 6™
	Wi-Fi CERTIFIED™ a, b, g, n, ac
Optimization	Wi-Fi Agile Multiband™
	WMM®

Certification ID: WFA83577

Date of Last Certification	January 21, 2020
Company	Hewlett Packard Enterprise
Product	Aruba Multiservice Mobility Controller/AP-535 Access Point
Model Number	AP-535

Source: <http://certifications.prod.wi-fi.org/pdf/certificate/public/download?cid=WFA73429>

WMM has been drafted in coordination with the 802.11e TG, and it is a subset of the QoS capabilities included in the 802.11e draft. WMM is based on the Enhanced Distributed Channel Access (EDCA) as defined by the 802.11e TG. The 802.11e draft

Source: <https://www.wi-fi.org/file/wi-fi-certified-for-wmm-2004>

10.22.2 HCF contention based channel access (EDCA)

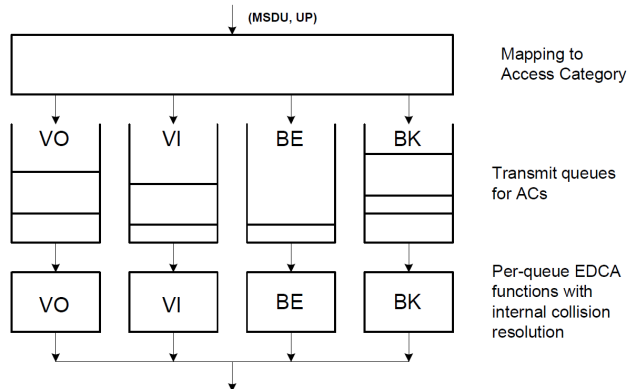


Figure 10-24—Reference implementation model when dot11AlternateEDCAActivated is false or not present

Source: IEEE Std 802.11-2016

Table 9-136—ACI-to-AC coding

ACI	AC	Description
0	AC_BE	Best effort
1	AC_BK	Background
2	AC_VI	Video
3	AC_VO	Voice

Source: IEEE Std 802.11-2016

10.2 MAC architecture

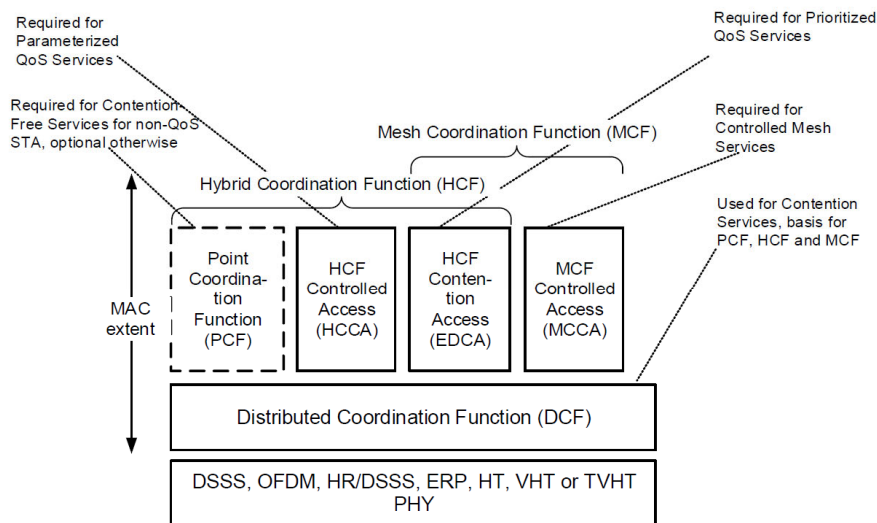


Figure 10-1—Non-DMG STA MAC architecture

Source: IEEE Std 802.11-2016

prioritized quality of service (QoS): The provisioning of service in which the medium access control (MAC) protocol data units (MPDUs) with higher priority are given a preferential treatment over MPDUs with a lower priority.

NOTE—Prioritized QoS is provided through the enhanced distributed channel access (EDCA) mechanism.

Source: IEEE Std 802.11-2016

10.2.4.2 HCF contention based channel access (EDCA)

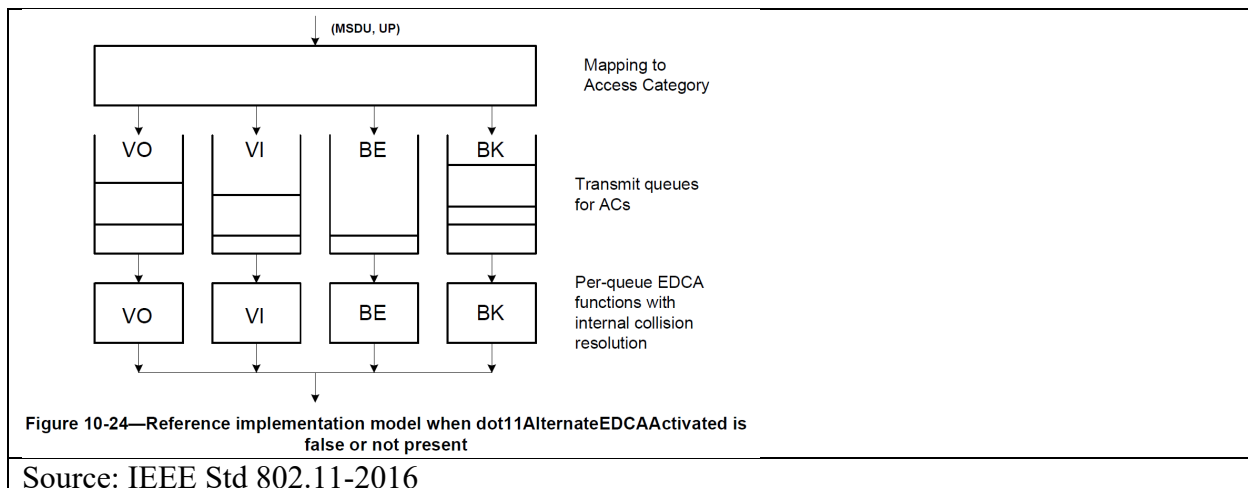
The EDCA mechanism provides differentiated, distributed access to the WM for STAs using eight different UPs. The EDCA mechanism defines four access categories (ACs) that provide support for the delivery of traffic with UPs at the STAs. Six transmit queues are defined when dot11AlternateEDCAActivated is true, and four transmit queues otherwise. The transmit queue and AC are derived from the UPs as shown in Table 10-1.

Source: IEEE Std 802.11-2016

frame: A unit of data exchanged between peer protocol entities.

user priority (UP): A value associated with an medium access control (MAC) service data unit (MSDU) that indicates how the MSDU is to be handled. The UP is assigned to an MSDU in the layers above the MAC.

Source: IEEE Std 802.11-2016



Source: IEEE Std 802.11-2016

58. The method practiced by the '318 Accused Products includes queuing data frames to be transmitted during a transmitting station's transmit opportunity, wherein the data frames are queued in a queue:

transmission opportunity (TXOP): An interval of time during which a particular quality-of-service (QoS) station (STA) has the right to initiate frame exchange sequences onto the wireless medium (WM).

NOTE—A TXOP is defined by a starting time and a maximum duration.

Source: IEEE Std 802.11-2016

4.5.2.3 QoS traffic scheduling

QoS traffic scheduling provides intra-BSS QoS frame transfers under the HCF, using either contention based or controlled channel access. At each TXOP, a traffic scheduling entity at the STA selects a frame for transmission, from the set of frames at the heads of a plurality of traffic queues, based on requested UP and/or parameter values in the traffic specification (TSPEC) for the requested MSDU. Additional information is available in 10.22.

Source: IEEE Std 802.11-2016

10.22 HCF

Under HCF, the basic unit of allocation of the right to transmit onto the WM is the TXOP. Each TXOP is defined by a starting time and a defined maximum length. In a non-DMG BSS, the TXOP may be obtained by a STA winning an instance of EDCA contention (see 10.22.2) during the CP or by a STA receiving a QoS (+)CF-Poll frame (see 10.22.3) during the CP or CFP. The former is called *EDCA TXOP*, while the latter is called *HCCA TXOP* or *polled TXOP*.

Source: IEEE Std 802.11-2016

10.22.2 HCF contention based channel access (EDCA)

10.22.2.1 Reference model

The EDCA channel access protocol is derived from the DCF procedures described in 10.3 by adding four independent enhanced distributed channel access functions (EDCAFs) to provide differentiated priorities to transmitted traffic, through the use of four different access categories (ACs).

For the case in which dot11AlternateEDCAActivated is false or not present, a model of the reference implementation is shown in Figure 10-24 and for the case in which dot11AlternateEDCAActivated is true, a model is shown in Figure 10-25. These figures illustrate a mapping from frame type or UP to the transmit queues and the four independent EDCAFs. The mapping of UP to the transmit queue and the mapping to AC are described in 10.2.4.2 and Table 10-1. The mapping of frame types to ACs is also described in 10.2.4.2.

Source: IEEE Std 802.11-2016

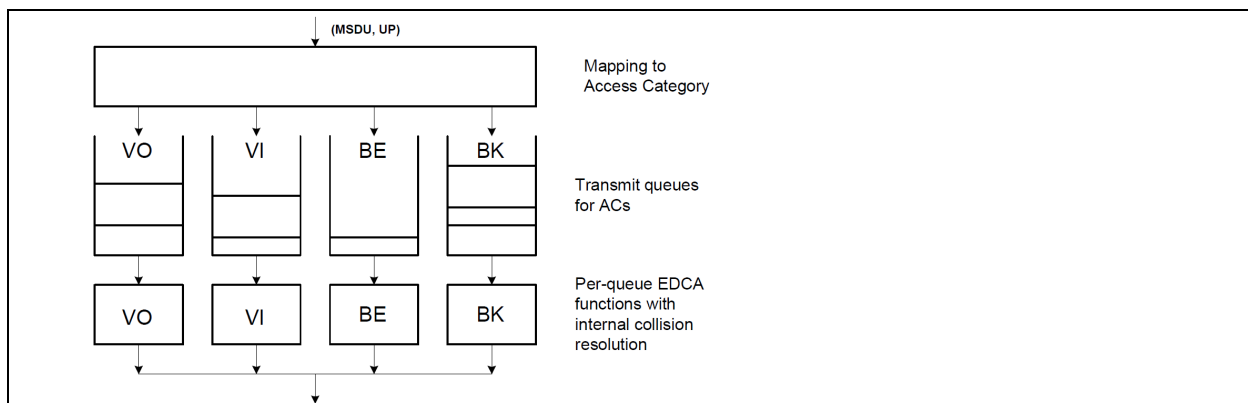


Figure 10-24—Reference implementation model when dot11AlternateEDCAActivated is false or not present

Source: IEEE Std 802.11-2016

59. The method practiced by the '318 Accused Products includes the transmit opportunity corresponding to a length of time during which the transmitting station will transmit data frames from the queue to a shared-communications channel:

transmission opportunity (TXOP): An interval of time during which a particular quality-of-service (QoS) station (STA) has the right to initiate frame exchange sequences onto the wireless medium (WM).

NOTE—A TXOP is defined by a starting time and a maximum duration.

Source: IEEE Std 802.11-2016

4.5.2.3 QoS traffic scheduling

QoS traffic scheduling provides intra-BSS QoS frame transfers under the HCF, using either contention based or controlled channel access. At each TXOP, a traffic scheduling entity at the STA selects a frame for transmission, from the set of frames at the heads of a plurality of traffic queues, based on requested UP and/or parameter values in the traffic specification (TSPEC) for the requested MSDU. Additional information is available in 10.22.

Source: IEEE Std 802.11-2016

10.22 HCF

Under HCF, the basic unit of allocation of the right to transmit onto the WM is the TXOP. Each TXOP is defined by a starting time and a defined maximum length. In a non-DMG BSS, the TXOP may be obtained by a STA winning an instance of EDCA contention (see 10.22.2) during the CP or by a STA receiving a QoS (+)CF-Poll frame (see 10.22.3) during the CP or CFP. The former is called *EDCA TXOP*, while the latter is called *HCCA TXOP* or *polled TXOP*.

Source: IEEE Std 802.11-2016

4.5.6 Traffic differentiation and QoS support

IEEE Std 802.11 uses a shared medium and provides differentiated control of access to the medium to handle data transfers with QoS requirements. The QoS facility (per MSDU traffic category and TSPEC negotiation) allows an IEEE 802.11 LAN to become part of a larger network providing end-to-end QoS delivery or to function as an independent network providing transport on a per-link basis with specified QoS commitments. The specifications regarding the integration and operability of the QoS facility with any other end-to-end QoS delivery mechanism like Resource Reservation Protocol (RSVP) are beyond the scope of this standard.

Source: IEEE Std 802.11-2016

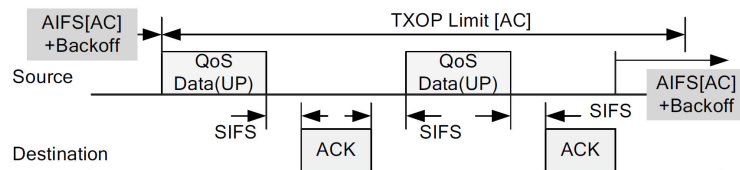


Figure 3.5 EDCA TXOP operation timing structure.

Source: Shorey, Rajeev, et al., eds. Mobile, wireless, and sensor networks: technology, applications, and future directions. John Wiley & Sons, 2006

60. The method practiced by the '318 Accused Products includes commencing the transmit opportunity with a control frame:

<p>9.2.5 Duration/ID field (QoS STA)</p> <p>9.2.5.2 Setting for single and multiple protection under enhanced distributed channel access (EDCA)</p> <p>In transmissions under EDCA by a STA that initiates a TXOP, there are two classes of duration settings: single protection and multiple protection. In single protection, the value of the Duration/ID field of the frame can set a network allocation vector (NAV) value at receiving STAs that protects up to the end of any following Data, Management, or response frame plus any additional overhead frames as described below. In multiple protection, the value of the Duration/ID field of the frame can set a NAV that protects up to the estimated end of a sequence of multiple frames.</p> <p>The STA selects between single and multiple protection when it transmits the first frame of a TXOP. All subsequent frames transmitted by the STA in the same TXOP use the same class of duration settings. A STA always uses multiple protection in a TXOP that includes:</p> <ul style="list-style-type: none"> — Frames that have the RDG/More PPDU subfield equal to 1 — PSMP frames — VHT NDP Announcement frames or Beamforming Report Poll frames <p>The Duration/ID field is determined as follows:</p> <ol style="list-style-type: none"> a) Single protection settings. <ol style="list-style-type: none"> 1) In an RTS frame that is not part of a dual clear-to-send (CTS) exchange, the Duration/ID field is set to the estimated time, in microseconds, required to transmit the pending frame, plus one CTS frame, plus one Ack or BlockAck frame if required, plus any NDPs required, plus explicit feedback if required, plus applicable IFSS. 2) In all CTS frames sent by STAs as the first frame in the exchange under EDCA and with the receiver address (RA) matching the MAC address of the transmitting STA, the Duration/ID field is set to one of the following: <ol style="list-style-type: none"> i) If there is a response frame, the estimated time required to transmit the pending frame, plus one SIFS, plus the response frame (Ack or BlockAck), plus any NDPs required, plus explicit feedback if required, plus an additional SIFS ii) If there is no response frame, the time required to transmit the pending frame, plus one SIFS <p>Source: IEEE Std 802.11-2016</p>
--

<p>9.3 Format of individual frame types</p> <p>9.3.1 Control frames</p> <p>9.3.1.2 RTS frame format</p> <p>9.3.1.3 CTS frame format</p> <p>Source: IEEE Std 802.11-2016</p>

61. The method practiced by the '318 Accused Products includes setting a length of time for the transmit opportunity:

10.2.4.2 HCF contention based channel access (EDCA)

The following rules apply for HCF contention based channel access:

- d) During an EDCA TXOP won by an EDCAF a STA may initiate multiple frame exchange sequences to transmit MMPDUs and/or MSDUs within the same AC. The duration of this EDCA TXOP is bounded, for an AC, by the value dot11QAPEDCATableTXOPLimit for an AP and by dot11EDCATableTXOPLimit for a non-AP STA. A value of 0 for this duration means that the EDCA TXOP is limited as defined by the rule for TXOP limit of 0 found in 10.22.2.8.

Source: IEEE Std 802.11-2016

```
dot11QAPEDCATableTXOPLimit OBJECT-TYPE
    SYNTAX Unsigned32 (0..65535)
    UNITS "32 microseconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "This is a control variable.
        It is written by an external management entity.
        Changes take effect as soon as practical in the implementation.

        This attribute specifies the maximum duration of an EDCA TXOP for a given
        AC, for an AP. The default value for this attribute is given (in different
        units) in Table 9-137.

        REFERENCE IEEE Std 802.11-2016, 9.4.2.29"
    ::= { dot11QAPEDCAEntry 5 }
```

Source: IEEE Std 802.11-2016

Table 9-137—Default EDCA Parameter Set element parameter values if dot11OCBAActivated is false

AC	CWmin	CWmax	AIFSN	TXOP limit			
				For PHYs defined in Clause 15 and Clause 16	For PHYs defined in Clause 17, Clause 18, Clause 19, and Clause 21	For PHY defined in Clause 22	Other PHYs
AC_BK	aCWmin	aCWmax	7	3.264 ms	2.528 ms	0	0
AC_BE	aCWmin	aCWmax	3	3.264 ms	2.528 ms	0	0
AC_VI	$(aCWmin+1)/2 - 1$	aCWmin	2	6.016 ms	4.096 ms	22.56 ms (BCU: 6 or 7 MHz), 16.92 ms (BCU: 8 MHz)	0
AC_VO	$(aCWmin+1)/4 - 1$	$(aCWmin+1)/2 - 1$	2	3.264 ms	2.080 ms	11.28 ms (BCU: 6 or 7 MHz), 8.46 ms (BCU: 8 MHz)	0

Source: IEEE Std 802.11-2016

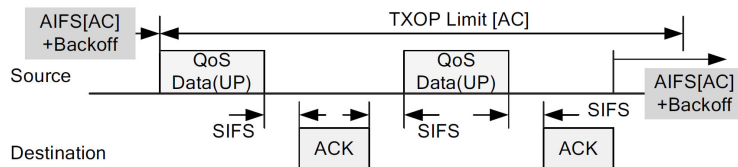


Figure 3.5 EDCA TXOP operation timing structure.

Source: Shorey, Rajeev, et al., eds. Mobile, wireless, and sensor networks: technology, applications, and future directions. John Wiley & Sons, 2006

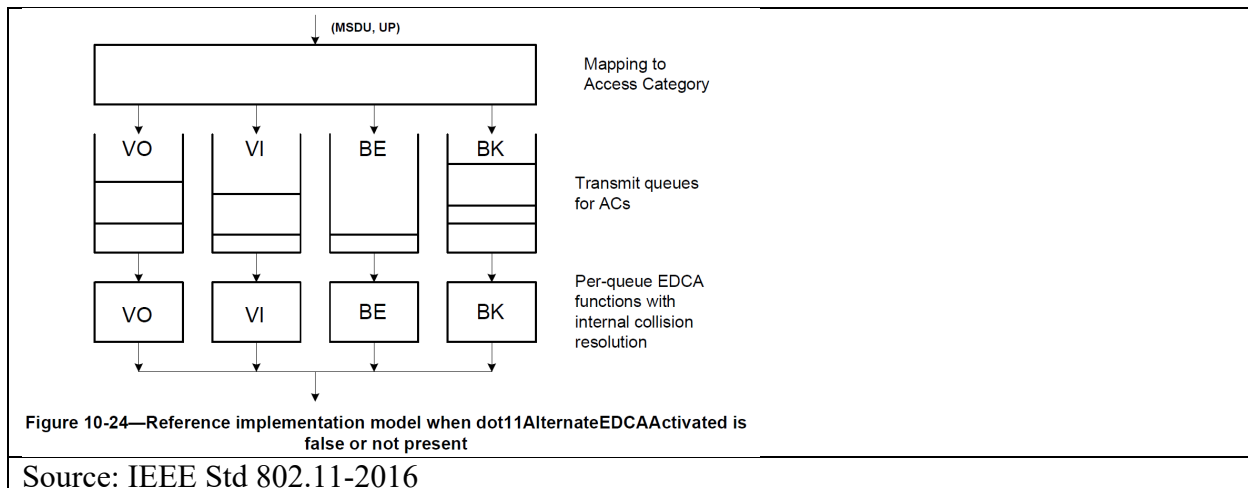
62. The method practiced by the '318 Accused Products includes setting the length of time for the transmit opportunity based on a priority of the queue:

10.2.4.2 HCF contention based channel access (EDCA)						
Table 10-1—UP-to-AC mappings						
Priority	UP (Same as IEEE 802.1D user priority)	IEEE 802.1D designation	AC	Transmit queue (dot11Alternate- EDCAActivated false or not present)	Transmit queue (dot11Alternate EDCAActivated true)	Designation (informative)
<div> <div>Lowest</div> <div>↓</div> <div>Highest</div> </div>	1	BK	AC_BK	BK	BK	Background
	2	—	AC_BK	BK	BK	Background
	0	BE	AC_BE	BE	BE	Best Effort
	3	EE	AC_BE	BE	BE	Best Effort
	4	CL	AC_VI	VI	A_VI	Video (alternate)
	5	VI	AC_VI	VI	VI	Video (primary)
	6	VO	AC_VO	VO	VO	Voice (primary)
	7	NC	AC_VO	VO	A_VO	Voice (alternate)

Source: IEEE Std 802.11-2016

Table 9-137—Default EDCA Parameter Set element parameter values if dot11OCBAActivated is false							
AC	CWmin	CWmax	AIFSN	TXOP limit			
				For PHYs defined in Clause 15 and Clause 16	For PHYs defined in Clause 17, Clause 18, Clause 19, and Clause 21	For PHY defined in Clause 22	Other PHYs
AC_BK	aCWmin	aCWmax	7	3.264 ms	2.528 ms	0	0
AC_BE	aCWmin	aCWmax	3	3.264 ms	2.528 ms	0	0
AC_VI	$(aCWmin+1)/2 - 1$	aCWmin	2	6.016 ms	4.096 ms	22.56 ms (BCU: 6 or 7 MHz), 16.92 ms (BCU: 8 MHz)	0
AC_VO	$(aCWmin+1)/4 - 1$	$(aCWmin+1)/2 - 1$	2	3.264 ms	2.080 ms	11.28 ms (BCU: 6 or 7 MHz), 8.46 ms (BCU: 8 MHz)	0

Source: IEEE Std 802.11-2016



63. HPE has had knowledge of the '318 patent since at least as early as the receipt of IV's presentation in April of 2022 presentation, which flagged the '318 patent; received further knowledge from IV's notice letter on November 13, 2022; and will receive further knowledge by service upon HPE of the Complaint in this Case.

64. Additionally, HPE has been, and currently is, an active inducer of infringement of the '318 patent under 35 U.S.C. § 271(b) and a contributory infringer of the '318 patent under 35 U.S.C. § 271(c).

65. HPE has actively induced, and continues to actively induce, infringement of the '318 patent by causing others to use, offer for sale, or sell products or services covered by the '318 patent, including the '318 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end-users, who, in turn, use, provision for use, offer for sale, or sell those products and services, which directly infringe the '318 patent. HPE's inducement includes the directions and instructions found at:

- https://www.arubanetworks.com/assets/ds/DS_AP530Series.pdf
- https://www.arubanetworks.com/techdocs/Instant_85_WebHelp/Content/instant-ug/voice-and-video/wmm-traffic-mgmt.htm

- https://support.hpe.com/hpesc/public/docDisplay?docId=a00073041en_us&docLocale=en_US

66. HPE has contributed to, and continues to contribute to, the infringement of the '318 patent by others by selling the '318 Accused Products, which, when installed, configured, and used directly infringe the '318 patent.

67. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe, and would actively induce and contribute to the infringement of, the '318 patent.

68. HPE has committed, and continues to commit, contributory infringement by selling products and services that directly infringe the '318 patent when used by a third party, such as the '318 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the '318 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

69. As a result of HPE's acts of infringement, Intellectual Ventures I has suffered and will continue to suffer damages in an amount to be determined at trial.

COUNTERCLAIM COUNT III

(HPE's Infringement of U.S. Patent No. 7,386,036)

70. The preceding paragraphs are incorporated by reference.

71. The '036 patent claims and teaches an improved multi-hop wireless system (*e.g.*, a mesh network) in which radio links between relays and user equipment are optimized separately from the links between relays and base stations. According to one embodiment, the methods and systems include transceivers of at least three kinds with at least two kinds of radio interfaces. The first kind of transceiver, a base station (BS), is connected to the core network. The second kind of transceiver, a relay station (RS), is connected to the BS with a first radio

interface, and to the third kind, the user equipment (UE), with a second radio interface. The first and second radio interfaces can operate, at least in part, using the same frequency bandwidth. Communication between relay station and the base station is processed separately from the communication between the user equipment and the base station.

72. As was known in the prior art, in the fourth-generation wireless systems (known as “4G” systems), capacities of 1 Gbps for a local area and 10 Mbps for wide area coverage were envisioned. However, even with very wide bandwidths on the order of 100 MHz, the spectral efficiencies needed for these capacities was extremely high. One way of achieving these spectral efficiencies was the use of multiple antennas to transmit and receive multiple simultaneous data streams, *i.e.* Multiple Input Multiple Output (“MIMO”) transmissions. Also, due to lack of free spectrum in the lower frequencies, carrier frequencies around 5 GHz were discussed. Even if the spectral efficiency requirements could be fulfilled, though, such systems would still have short ranges, due to the attenuation of high frequency signals. This combined with the limitations on transmit power and the requirements for high data rates, made communication cell ranges small, thus increasing the overall cost of the network. To combat the problem of small cell ranges, researchers proposed the use of a multi-hop network architecture.

73. Even with multi-hop relays, however, the combination of very high data rates and wide area coverage was still a problem. Multiple antennas could be used at the relays to increase the range to the next relay or base station or to increase the data rate, but to achieve both simultaneously was not an easy task. Capacity of the channel gave the maximum data rates which were possible to transmit reliably over the channel. However, in practical systems, a discrete set of modulations was used, and the maximum data rate could be limited by the modulations rather than the capacity. Higher order modulations, such as quadrature amplitude

modulation (“M-QAM”), where the cardinality of the modulation M is high, could not be used in practical systems. As the cardinality of the modulation increased, the transmission became less reliable. This could be compensated either by increasing the transmit power or by using a more complex receiver. But since the transmit power was limited and the cost of implementation of the receiver needed to be kept as low as possible, there was a strict upper limit for the cardinality of the modulation.

74. In light of the above, the inventors of the ’036 patent recognized the need for improved high data rate transmission in MIMO networks. Further, they recognized the need for a wireless multi-hop system with macroscopic multiplexing. And, they recognized the need to achieve high data rates in wireless communication systems at relatively low costs. The inventors of the ’036 patent thus recognized the need for optimizing separate links between the base station, multiple relay stations and user equipment.

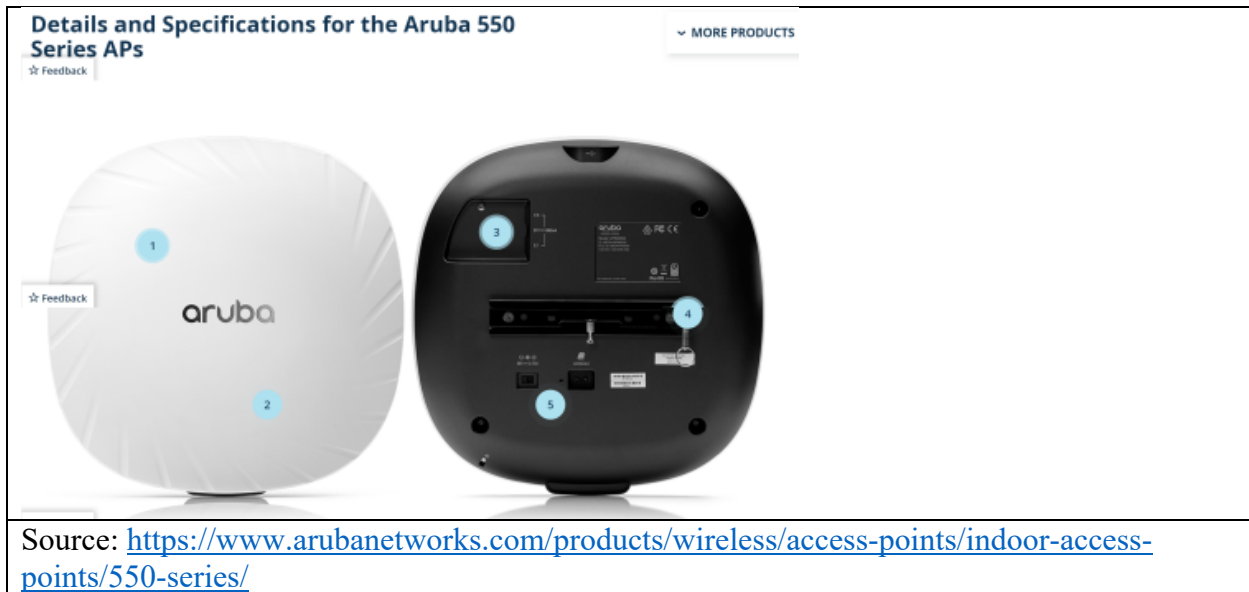
75. HPE has directly infringed and continues to directly infringe at least claim 11 of the ’036 patent by making, using, selling, offering for sale, and importing products and services covered by that patent’s claims. HPE’s products and services that infringe the ’036 patent include the line of access points (AP) with tri-radio operation, including at least the Aruba 550 and 555 series running ArubaOS 8.6.0.0 and above; and all other Aruba access point products or components (ArubaOS 8.6.0.0) which include in tri-radio operation made, used, sold, or offered for sale by or on behalf of HPE (collectively, “the ’036 Accused Products”).

76. Claim 11 of the ’036 patent is reproduced below:

11. A wireless communication system having a base station and a relay station that communicate with user equipment, the system comprising:
a base station having a first radio transceiver and being connected to a core network; and
a first relay station having a second radio transceiver and being configured to simultaneously communicate with the base station and with a second relay

station using a first radio interface and being configured to communicate with user equipment having a third radio transceiver using a second radio interface, wherein the operation of the first radio interface and the second radio interface are separate from each other.

77. The '036 Accused Products are a wireless communication system having a base station and a relay station that communicate with user equipment. A network comprising two or more Aruba 550 Series AP with ArubaOS 8.6.0.0 is one example, as seen below:



Tri-Radio Mode for 550 Series Access Points

Starting from ArubaOS 8.6.0.0, 550 Series access points support 802.11ax 8x8 dual-radio with optional 4x4 tri-radio operating mode. In tri-radio mode or split 5 GHz mode, 8x8:8SS 5 GHz radio is split into dual 4x4:4SS 5 GHz radio. The two radios can work on AP mode and also work on AP+AM or AP+ Spectrum mode, where one radio provides wireless access and the other radio performs scanning. Tri-radio mode works only under BT POE or DC power. The operations on the 5 GHzband is split and carried out by two separate radios— lower 5 GHz radio and upper 5 GHz radio. The lower 5 GHz radio operates on channels 32–64 and the upper 5 GHz radio operates on channels 100–173. The Tri-radio mode in 550 Series Access Points supports the following features:

Source:

https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/access-points/tri-radio-mode.htm

Secure Enterprise Mesh

The Aruba secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. Using mesh, you can bridge multiple Ethernet LANs or you can extend your wireless coverage. As traffic

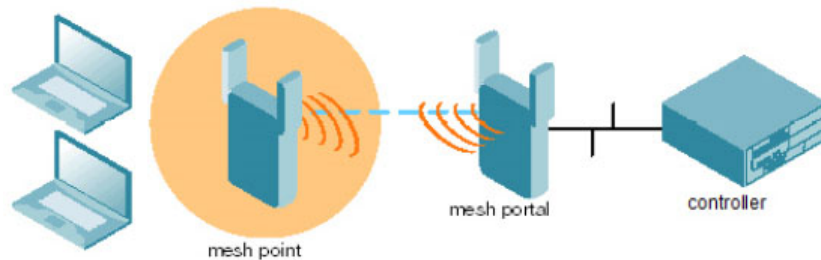
Source: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/secu-ente-mesh.htm

Understanding Mesh Access Points

Mesh APs learn about their environment when they boot up. Mesh APs are either configured as a mesh portal (MPP), an AP that uses its wired interface to reach the controller, or a mesh point (MP), an AP that establishes an all-wireless path to the mesh portal. Mesh APs locate and associate with their nearest neighbor, which

Source:

https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Mesh/Mesh_Access_Points.htm



Source: https://www.arubanetworks.com/techdocs/ArubaOS_60/UserGuide/Mesh.php

78. In the '036 Accused Products, the wireless communication system has a base station having a first radio transceiver and being connected to a core network:

Aruba 550 Series

AP type: Indoor, dual/tri-radio, 5GHz and 2.4GHz 802.11ax 4x4 MIMO

5GHz radio (dual-radio operation): Eight spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate with individual 8SS HE80 (or 4SS HE160) 802.11ax client devices, or with eight 1SS or four 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously

5GHz radio (tri-radio operation): Four spatial stream Single User (SU) MIMO for up to 2.4Gbps wireless data rate with individual 4SS HE80 (or 2SS HE160) 802.11ax client devices, or with four 1SS or two 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously

2.4GHz radio: Four spatial stream Single User (SU) MIMO for up to 1,150Mbps wireless data rate with individual 4SS HE40 802.11ax client devices or with two 2SS HE40 802.11ax MU-MIMO capable client devices simultaneously

Source: <https://www.arubanetworks.com/products/networking/access-points/550-series/>

Aruba Networks AP-555 (APIN0555)

WI1 chip1: Qualcomm QCN5154

WI1 chip2: Qualcomm QCN5154

WI1 802dot11 protocols: an+ac+ax

WI1 MIMO config: 8x8:8

WI1 antenna connector: none

WI2 chip1: Qualcomm QCN5124

WI2 802dot11 protocols: bgn+ax

WI2 MIMO config: 4x4:4

Source: [https://wikidevi.wi-cat.ru/Aruba_Networks_AP-555_\(APIN0555\)](https://wikidevi.wi-cat.ru/Aruba_Networks_AP-555_(APIN0555))

By default, APs operate as thin APs, which means their primary function is to receive and transmit electromagnetic signals; other WLAN processing is left to the controller. When planning a mesh network, you manually configure APs to operate in mesh portal or mesh point roles. Unlike a traditional WLAN Mesh APs learn about their environment when they boot up. Mesh APs are either configured as a mesh portal (MPP), an AP that uses its wired interface to reach the controller, or a mesh point (MP), an AP that establishes an all-wireless path to the mesh portal. Mesh APs locate and associate with their nearest

Source:

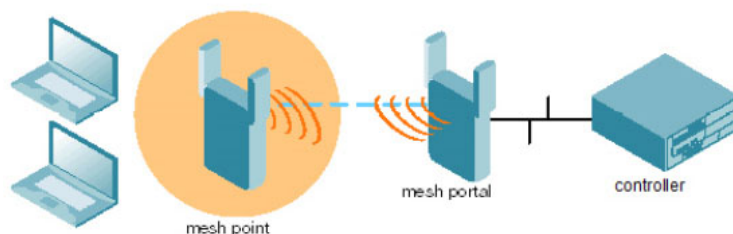
https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyle/s/Mesh/Mesh_Access_Points.htm

Mesh Portals

The mesh portal (MPP) is the gateway between the wireless mesh network and the enterprise wired LAN. You configure an Aruba AP to perform the mesh portal role, which uses its wired interface to establish a link to the wired LAN. You can deploy multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

Source:

https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyle/s/Mesh/Mesh_Access_Points.htm



Source: https://www.arubanetworks.com/techdocs/ArubaOS_60/UserGuide/Mesh.php

79. In the '036 Accused Products, the wireless communication system has a first relay station having a second radio transceiver:

<p>Aruba 550 Series</p> <p>AP type: Indoor, dual/tri-radio, 5GHz and 2.4GHz 802.11ax 4x4 MIMO</p> <p>5GHz radio (dual-radio operation): Eight spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate with individual 8SS HE80 (or 4SS HE160) 802.11ax client devices, or with eight 1SS or four 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously</p> <p>5GHz radio (tri-radio operation): Four spatial stream Single User (SU) MIMO for up to 2.4Gbps wireless data rate with individual 4SS HE80 (or 2SS HE160) 802.11ax client devices, or with four 1SS or two 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously</p> <p>2.4GHz radio: Four spatial stream Single User (SU) MIMO for up to 1,150Mbps wireless data rate with individual 4SS HE40 802.11ax client devices or with two 2SS HE40 802.11ax MU-MIMO capable client devices simultaneously</p> <p>Source: https://www.arubanetworks.com/products/networking/access-points/550-series/</p>
--

<p>Aruba Networks AP-555 (APIN0555)</p> <p>WI1 chip1: Qualcomm QCN5154</p> <p>WI1 chip2: Qualcomm QCN5154</p> <p>WI1 802dot11 protocols: an+ac+ax</p> <p>WI1 MIMO config: 8x8:8</p> <p>WI1 antenna connector: none</p> <p>WI2 chip1: Qualcomm QCN5124</p> <p>WI2 802dot11 protocols: bgn+ax</p> <p>WI2 MIMO config: 4x4:4</p> <p>Source: https://wikidevi.wi-cat.ru/Aruba_Networks_AP-555_(APIN0555)</p>

<p>By default, APs operate as thin APs, which means their primary function is to receive and transmit electromagnetic signals; other WLAN processing is left to the controller. When planning a mesh network, you manually configure APs to operate in mesh portal or mesh point roles. Unlike a traditional WLAN</p> <p>Mesh APs learn about their environment when they boot up. Mesh APs are either configured as a mesh portal (MPP), an AP that uses its wired interface to reach the controller, or a mesh point (MP), an AP that establishes an all-wireless path to the mesh portal. Mesh APs locate and associate with their nearest</p> <p>Source: https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyle/s/Mesh/Mesh_Access_Points.htm</p>
--

80. In the '036 Accused Products, the wireless communication system has a first relay station configured to simultaneously communicate with the base station and with a second relay

station using a first radio interface and being configured to communicate with user equipment having a third radio transceiver using a second radio interface:

Secure Enterprise Mesh

The Aruba secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. Using mesh, you can bridge multiple [Ethernet](#) LANs or you can extend your wireless coverage. As traffic

Source: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/secu-ente-mesh.htm

Overview of Mesh Access Points

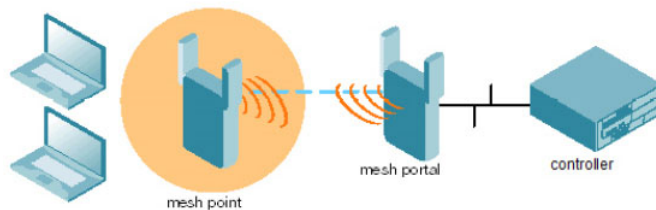
Mesh APs learn about their environment when they boot up. Mesh APs are either configured as a mesh portal, an AP that uses its wired interface to reach the managed device, or a mesh point, an AP that establishes an all-wireless path to the mesh portal. Mesh APs locate and associate with their nearest neighbor, which provides the best path to the mesh portal. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe APs configured for mesh.

Source: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/mesh_aps.htm

Overview of Mesh Links

The mesh link is the data link between a mesh point and its parent. A mesh point uses the parameters defined in the mesh cluster profile, to establish a mesh link with a neighboring mesh point. The mesh link uses a series of metrics to establish the best path to the mesh portal.

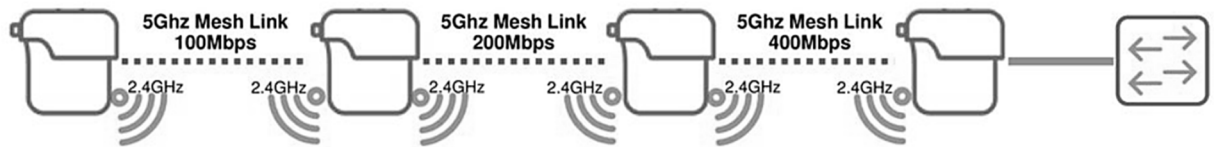
Source: https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/unde-mesh-link.htm



Source: https://www.arubanetworks.com/techdocs/ArubaOS_60/UserGuide/Mesh.php

Single-Channel Multi-hop Mesh

Multiple points will build mesh links, or 'hops' to other points to extend the mesh using the same 5GHz radio on each point, in a hop-by-hop fashion



Source: <https://slideplayer.com/slide/13652141>

Aruba 550 Series

AP type: Indoor, dual/tri-radio, 5GHz and 2.4GHz 802.11ax 4x4 MIMO

5GHz radio (dual-radio operation): Eight spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate with individual 8SS HE80 (or 4SS HE160) 802.11ax client devices, or with eight 1SS or four 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously

5GHz radio (tri-radio operation): Four spatial stream Single User (SU) MIMO for up to 2.4Gbps wireless data rate with individual 4SS HE80 (or 2SS HE160) 802.11ax client devices, or with four 1SS or two 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously

2.4GHz radio: Four spatial stream Single User (SU) MIMO for up to 1,150Mbps wireless data rate with individual 4SS HE40 802.11ax client devices or with two 2SS HE40 802.11ax MU-MIMO capable client devices simultaneously

Source: <https://www.arubanetworks.com/products/networking/access-points/550-series/>

81. In the '036 Accused Products, the wireless communication system has the operation of the first radio interface and the second radio interface separate from each other:

Aruba 550 Series

WI-FI RADIO SPECIFICATIONS

The 550 Series is designed to simultaneously serve multiple clients and traffic types with dual radio (8x8 + 4x4 MIMO) and optional tri-radio mode, boosting overall network performance by up to 4X versus 802.11ac APs.

AP type: Indoor, dual/tri-radio, 5GHz and 2.4GHz 802.11ax 4x4 MIMO

5GHz radio (dual-radio operation): Eight spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate with individual 8SS HE80 (or 4SS HE160) 802.11ax client devices, or with eight 1SS or four 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously

5GHz radio (tri-radio operation): Four spatial stream Single User (SU) MIMO for up to 2.4Gbps wireless data rate with individual 4SS HE80 (or 2SS HE160) 802.11ax client devices, or with four 1SS or two 2SS HE80 802.11ax MU-MIMO capable client devices simultaneously

2.4GHz radio: Four spatial stream Single User (SU) MIMO for up to 1,150Mbps wireless data rate with individual 4SS HE40 802.11ax client devices or with two 2SS HE40 802.11ax MU-MIMO capable client devices simultaneously

Source: <https://www.arubanetworks.com/products/networking/access-points/550-series/>

Tri-Radio Mode for 550 Series Access Points

Starting from ArubaOS 8.6.0.0, 550 Series Access points will support 802.11ax 8x8 dual-radio with optional 4x4 tri-radio operating mode.

In tri-radio mode or split 5GHz mode, 8x8:8SS 5GHz radio is split into dual 4x4:4SS 5GHz radio. The two radios can work on AP mode and also work on AP+AM or AP+ Spectrum mode, where one radio provides wireless access and the other radio performs scanning. Tri-radio mode works only under BT POE or DC power.

The Tri-radio mode in 550 Series Access Points supports the following features:

- Station Management
- AirMatch
- SAPD/SAPM
- Spectrum Analysis
- Cluster
- MultiZone
- Mesh
- ClientMatch
- Firmware

Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/tri-radio-mode.htm

82. HPE has had knowledge of the '036 patent since at least as early as the receipt of IV's presentation in April of 2022 presentation, which flagged the '036 patent; received further knowledge from IV's notice letter on November 13, 2022; and will receive further knowledge by service upon HPE of the Complaint in this Case.

83. Additionally, HPE has been, and currently is, an active inducer of infringement of the '036 patent under 35 U.S.C. § 271(b) and a contributory infringer of the '036 patent under 35 U.S.C. § 271(c).

84. HPE has actively induced, and continues to actively induce, infringement of the '036 patent by causing others to use, offer for sale, or sell products or services covered by the '036 patent, including the '036 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end-users, who, in turn, use, provision for use, offer for sale, or sell those products and services, which directly infringe the '036 patent. HPE's inducement includes the directions and instructions found at:

- <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/550-series/>
- https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/access-points/tri-radio-mode.htm

- https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/secu-ente-mesh.htm
- https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Mesh/Mesh_Access_Points.htm
- https://www.arubanetworks.com/techdocs/ArubaOS_60/UserGuide/Mesh.php
- https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/mesh_aps.htm
- https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/mesh/unde-mesh-link.htm
- https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/tri-radio-mode.htm

85. HPE has contributed to, and continues to contribute to, the infringement of the '036 patent by others by selling the '036 Accused Products, which, when installed, configured, and used directly infringe the '036 patent.

86. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe, and would actively induce and contribute to the infringement of, the '036 patent.

87. HPE has committed, and continues to commit, contributory infringement by selling products and services that directly infringe the '036 patent when used by a third party, such as the '036 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the '036 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

88. As a result of HPE's acts of infringement, Intellectual Ventures I has suffered and will continue to suffer damages in an amount to be determined at trial.

COUNTERCLAIM COUNT IV

(HPE's Infringement of U.S. Patent No. 8,594,122)

89. The preceding paragraphs are incorporated by reference.

90. The '122 patent claims and teaches methods and systems for wireless network communication. According to one embodiment, a transmitter is configured to transmit a first communication frame from a first station to a second station; and provide a transmit announcement indication in the first communications frame, the transmit announcement indication indicating whether a second communication frame to the second station will follow the first communication frame.

91. As was known in the prior art, as communication devices became smaller, while also providing increasing functionality, increasing transmission speed without dramatically affecting overhead raised significant design challenges. Such novel methods and systems were disclosed in the '122 patent.

92. HPE has directly infringed and continues to directly infringe at least claim 1 of the '122 patent by making, using, selling, offering for sale, and importing products and services covered by that patent's claims. HPE's products and services that infringe the '122 patent include at least all Aruba 802.11 access points ("AP") that support 802.11ac; and all other Aruba APs or components (including ArubaOS) that support beamforming, made, used, sold, or offered for sale by or on behalf of HPE (collectively, "the '122 Accused Products").

93. Claim 1 of the '122 patent is reproduced below:

1. A method comprising:

transmitting a first communication frame from a first station to a second station;

wherein the first communication frame comprises an address of the second station and a transmit announcement indication indicating that a second communication frame intended for the second station will follow the first communication frame and that the second communication frame will not

include the address of the second station, and wherein the second communication frame follows after a short inter frame space (SIFS) after the first communication frame with the transmit announcement indication.

94. The '122 Accused Products perform a method of communication. The AP-535

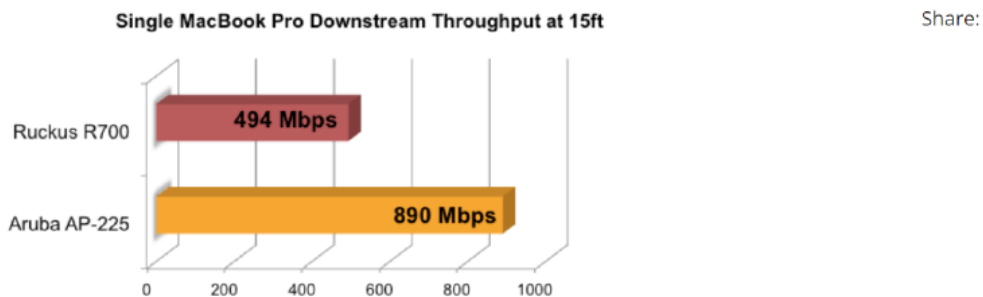
AP is one example, which implements 802.11ac as seen below:

Aruba's standards-based beamforming implementation involves a constant exchange of information between the client and AP to maximize the client receive signal. This is critical for improving wireless performance in dynamic RF environments with highly mobile clients.


All Aruba 802.11ac APs support standards-beamforming, thanks to Broadcom. Just about every 802.11ac device, including the Samsung Galaxy S4, MacBook Pro and MacBook Air, support beamforming. So we actually have a solution that works on the network *and* the client side.

We compared Aruba's 802.11ac beamforming against non-standard beamforming in a simple rate-vs.-range test. The other vendor's performance at 15 feet is equal to Aruba's performance at 120 feet.

Standard 802.11ac beamforming wins hands down.



Source: <https://blogs.arubanetworks.com/solutions/11ac-beamforming-makes-the-dog-rollover/>



The worldwide network of companies that brings you Wi-Fi®

Certified products, news, etc.

SEARCH

View Wi-Fi CERTIFIED™ products by category

CSV Download your results

SHOW NAVIGATION

Product Finder

Filtered Results

Clear all filters

Keyword Search

ADD

Brand

×

Hewlett Packard Enterprise

Categories

☐ Building

☐ Computers & Accessories

☐ Gaming, Media & Music

☐ Phones

☐ Routers

☐ Smart Home

☐ Tablets, Ereaders & Cameras

☐ Televisions & Set Top Boxes

☐ Other

Featured Capabilities

☐ Miracast®

☐ Wi-Fi CERTIFIED 6™

☒ Wi-Fi CERTIFIED™ ac

☐ Wi-Fi Easy Connect™

☐ Wi-Fi EasyMesh™

☐ Wi-Fi Home Design™

☐ Wi-Fi Vantage™

☐ WPA3™-Enterprise


☐ WPA3™-Personal

Hide Advanced Filters

All Capabilities

Connectivity

Security



Product Name:

AP615

Model Number:

AP615

Total Variants:

2 (2 results)

Brand:


Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-10-14



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-505

Total Variants:

5 (5 results)

Brand:


Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-10-14



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-515

Total Variants:

5 (5 results)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-10-14



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-587

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-06-29



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-584

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-06-29



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-585

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-06-09



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-535

Total Variants:

5 (5 results)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-06-01



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-655

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-03-30



Product Name:

Aruba Instant On AP25 Ac...

Model Number:

AP25

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2022-03-18



Product Name:

Aruba Multiservice Mobili...

Model Number:

AP-635

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise

Category:

Routers

Last Certified Date:

2021-12-16



Product Name:

Aruba Instant On AP17 Ac...

Model Number:

AP17

Total Variants:

1 (1 result)

Brand:

Hewlett Packard Enterprise



Product Name:

Aruba Instant On AP15 Ac...

Model Number:

AP15

Total Variants:


1 (1 result)

Brand:


Hewlett Packard Enterprise

Source: https://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&capabilities=235&companies=301


All Capabilities
Connectivity
Security
Optimization
Access
Applications & Services
Wi-Fi & Cellular Radio Coexistence
Spectrum & Regulatory Features
Additional Capabilities
Date Certified
from
to




Product Name: Aruba Instant On AP17 Ac...
Model Number: AP17
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2021-07-09




Product Name: Aruba Instant On AP15 Ac...
Model Number: AP15
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2021-07-09




Product Name: Aruba Instant On AP12 Ac...
Model Number: AP12
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2021-07-09




Product Name: Aruba Instant On AP11D ...
Model Number: AP11D
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2021-07-09




Product Name: Aruba Instant On AP11 Ac...
Model Number: AP11
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2021-07-08




Product Name: Aruba Multiservice Mobili...
Model Number: AP-567
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-08-10




Product Name: Aruba Multiservice Mobili...
Model Number: AP-565
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-08-10




Product Name: Aruba Multiservice Mobili...
Model Number: AP-503H
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-07-21




Product Name: Aruba Multiservice Mobili...
Model Number: AP-518
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-05-29




Product Name: Aruba Multiservice Mobili...
Model Number: AP 504
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-05-20




Product Name: Aruba Instant On AP22 Ac...
Model Number: AP22
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-05-04



Product Name: Aruba Multiservice Mobili...
Model Number: AP-505H
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-04-28















Product Name: Aruba Multiservice Mobili...
Model Number: AP-574
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-04-14



Product Name: Aruba Multiservice Mobili...
Model Number: AP-577
Total Variants: 1 (1 result)
Brand: Hewlett Packard Enterprise
Category: Routers
Last Certified Date: 2020-04-14


Source: https://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&capabilities=235&companies=301

 Model Number: AP-518 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-05-29	 Model Number: AP 504 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-05-20
 Product Name: Aruba Instant On AP22 Ac... Model Number: AP22 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-05-04	 Product Name: Aruba Multiservice Mobili... Model Number: AP-505H Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-04-28
 Product Name: Aruba Multiservice Mobili... Model Number: AP-574 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-04-14	 Product Name: Aruba Multiservice Mobili... Model Number: AP-577 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-04-14
 Product Name: Aruba Multiservice Mobili... Model Number: AP-575 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-04-14	 Product Name: Aruba Multiservice Mobili... Model Number: AP-555 Total Variants: 4 (4 results) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-01-21
 Product Name: Aruba Multiservice Mobili... Model Number: AP-534 Total Variants: 4 (4 results) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-01-21	 Product Name: Aruba Multiservice Mobili... Model Number: AP-514 Total Variants: 4 (4 results) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-01-20
 Product Name: Aruba Instant Access Poin... Model Number: AP-515 Total Variants: 4 (4 results) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-01-20	 Product Name: Aruba Instant Access Poin... Model Number: AP-514 Total Variants: 4 (4 results) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2020-01-20


[TERMS OF USE](#)
[PRIVACY POLICY](#)
[CAREERS](#)
[CONTACT US](#)
[VULNERABILITY REPORTING](#)

© 2022 Wi-Fi Alliance. All rights reserved.
 Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, and other marks are trademarks of Wi-Fi Alliance.

Source: https://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&capabilities=235&companies=301

Featured Capabilities <ul style="list-style-type: none"> <input type="checkbox"/> Miracast® <input type="checkbox"/> Wi-Fi CERTIFIED 6™ <input checked="" type="checkbox"/> Wi-Fi CERTIFIED™ ac <input type="checkbox"/> Wi-Fi Easy Connect™ 	 Product Name: Aruba Multiservice Mobili... Model Number: AP-535 Total Variants: 5 (5 results) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2022-06-01
---	---

Source: https://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&capabilities=235&companies=301



Specifications

Hardware Variants ^

AP-534: External antenna models
AP-535: Internal antenna models

802.11ac very high throughput (VHT) support: VHT20/40/80/160

Transmit beam-forming (TxBF) for increased signal reliability and range

Source: <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/530-series/>

IEEE Std 802.11™-2016 (Revision of IEEE Std 802.11-2012)

10.34.5 VHT sounding protocol

10.34.5.1 General

Transmit beamforming and DL-MU-MIMO require knowledge of the channel state to compute a steering matrix that is applied to the transmitted signal to optimize reception at one or more receivers. The STA transmitting using the steering matrix is called the *VHT beamformer*, and a STA for which reception is optimized is called a *VHT beamformee*. An explicit feedback mechanism is used where the VHT beamformee directly measures the channel from the training symbols transmitted by the VHT beamformer and sends back a transformed estimate of the channel state to the VHT beamformer. The VHT beamformer then uses this estimate, perhaps combining estimates from multiple VHT beamformees, to derive the steering matrix.

10.34.5.2 Rules for VHT sounding protocol sequences

A VHT beamformer shall initiate a sounding feedback sequence by transmitting a VHT NDP Announcement frame followed by a VHT NDP after a SIFS. The VHT beamformer shall include in the VHT NDP Announcement frame one STA Info field for each VHT beamformee that is expected to prepare VHT Compressed Beamforming feedback and shall identify the VHT beamformee by including the VHT beamformee's AID in the AID subfield of the STA Info field. The VHT NDP Announcement frame shall include at least one STA Info field.

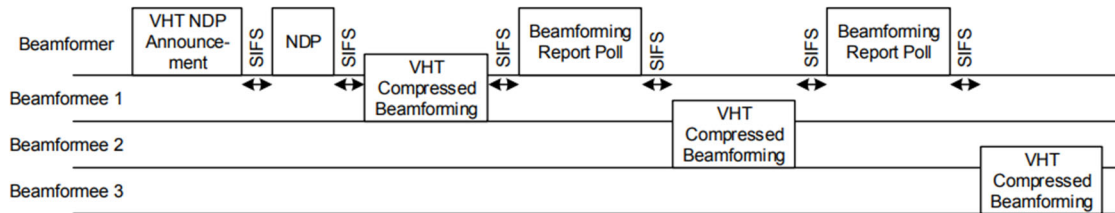


Figure 10-53—Example of the sounding protocol with more than one VHT beamformee

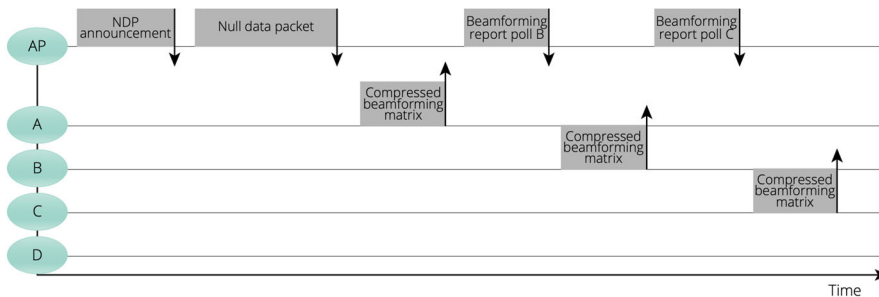
Source: IEEE Std 802.11-2016

Sounding frames in 802.11ac

802.11n included three options for beamforming feedback, and manufacturers have not been able to agree and implement a common set. In practice, some current 802.11n devices will successfully beamform when both ends of the connection include common chipsets, but beamforming with explicit feedback is not generally a feature of current 802.11n equipment.

To avoid this situation, only one feedback mechanism, explicit feedback with the compressed V matrix is specified in 802.11ac. The full sounding sequence comprises a set of special sounding frames sent by the transmitter (either the beamformer or the access point in the case of DL MU-MIMO), and a set of compressed V matrix frames returned by the beamformee. Because multiple clients are involved in MU-MIMO, a special protocol ensures they answer with feedback frames in sequence following the sounding frame.

In 802.11ac, the protocol for generating CSI at the transmitter relies on sounding or null data packet (NDP) frames, together with announcement frames and response frames.



Source: https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf

95. The method practiced by the '122 Accused Products includes transmitting a first communication frame from a first station to a second station, wherein the first communication frame comprises an address of the second station:

10.34.5.2 Rules for VHT sounding protocol sequences

A VHT beamformer shall initiate a sounding feedback sequence by transmitting a VHT NDP Announcement frame followed by a VHT NDP after a SIFS. The VHT beamformer shall include in the VHT NDP Announcement frame one STA Info field for each VHT beamformee that is expected to prepare VHT Compressed Beamforming feedback and shall identify the VHT beamformee by including the VHT beamformee's AID in the AID subfield of the STA Info field. The VHT NDP Announcement frame shall include at least one STA Info field.

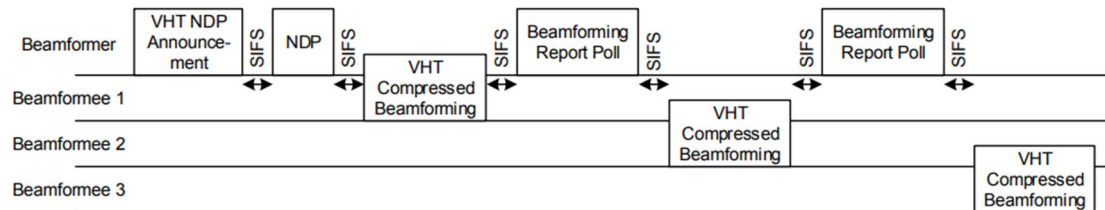


Figure 10-53—Example of the sounding protocol with more than one VHT beamformee

Source: IEEE Std 802.11-2016

9.3.1.20 VHT NDP Announcement frame format

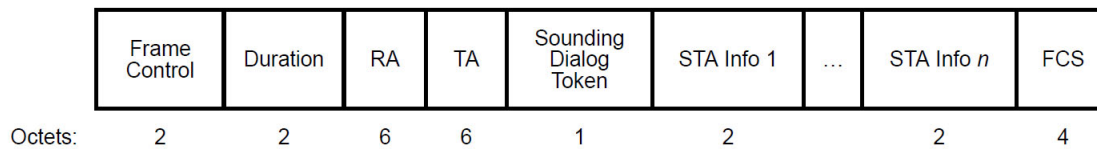


Figure 9-49—VHT NDP Announcement frame format

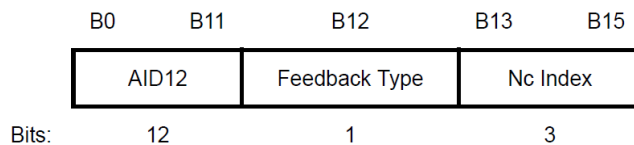


Figure 9-51—STA Info field

Table 9-25—STA Info subfields

Field	Description
AID12	Contains the 12 least significant bits of the AID of a STA expected to process the following VHT NDP and prepare the sounding feedback. Equal to 0 if the STA is an AP, mesh STA, or STA that is a member of an IBSS.

9.4.1.8 AID field

In infrastructure BSS operation, the AID field contains a value assigned by an AP or PCP during association. The field represents the 16-bit ID of a STA. In mesh BSS operation, the AID field is a value that represents the

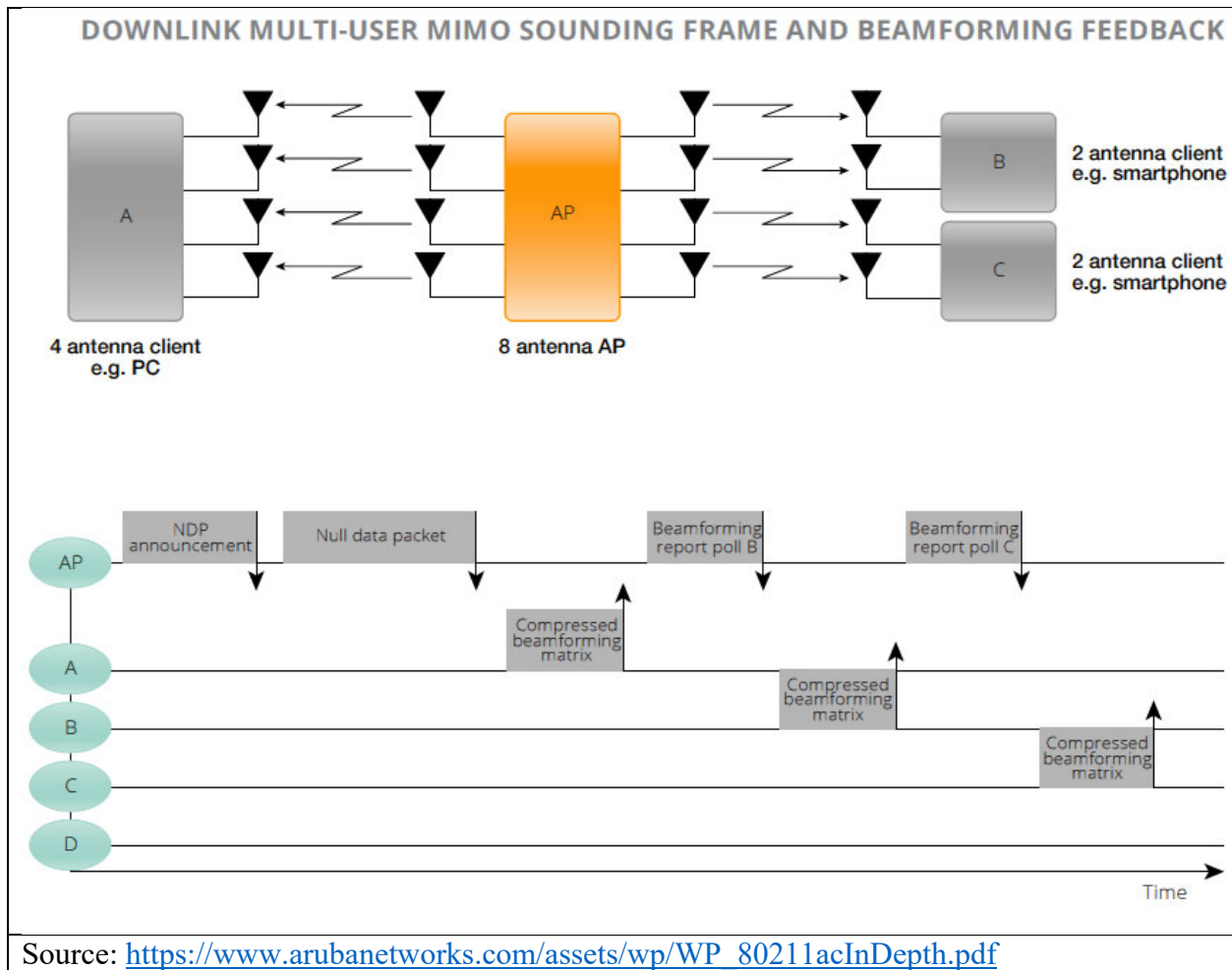
Source: IEEE Std 802.11-2016

First, the beamformer sends a null data packet announcement (NDPA) frame identifying the intended recipients and the format of the forthcoming sounding frame. This is followed by the sounding NDP itself, and the beamformee then responds with a beamforming report frame.

The NDPA and NDP frames are quite simple. The NDPA identifies which stations should listen to the subsequent sounding frame, along with the dimensions of that frame depending on the number of antennas and spatial streams in use. The sounding frame itself is just a null data packet: It is the preamble with its LTFs that is of importance. The processing and construction of the beamforming report, however, is complicated.

To allow clients to quickly identify if a frame is addressed to them, a new field called partial association ID (partial AID) or Group ID for MU-MIMO is added to the preamble. If the partial AID field is not its own address, the client can doze for the remainder of the TXOP.

Source: https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf



96. The method practiced by the '122 Accused Products includes the first communication frame comprises a transmit announcement indication indicating that a second communication frame intended for the second station:

10.20 Group ID and partial AID in VHT PPDU

The partial AID is a nonunique STA identifier defined in Table 10-9. The partial AID is carried in the TXVECTOR parameter PARTIAL_AID of a VHT SU PPDU and is limited to 9 bits.

A STA transmitting a VHT SU PPDU carrying one or more group addressed MPDUs or transmitting a VHT NDP intended for multiple recipients shall set the TXVECTOR parameters GROUP_ID to 63 and PARTIAL_AID to 0. The intended recipient of a VHT NDP is defined in 10.34.6.

Source: IEEE Std 802.11-2016

10.34.6 Transmission of a VHT NDP

The destination of a VHT NDP is equal to the RA of the immediately preceding VHT NDP Announcement frame.

Source: IEEE Std 802.11-2016

10.34.5.2 Rules for VHT sounding protocol sequences

If the VHT NDP Announcement frame includes more than one STA Info field, the RA of the VHT NDP Announcement frame shall be set to the broadcast address. If the VHT NDP Announcement frame includes a single STA Info field, the RA of the VHT NDP Announcement frame shall be set to the MAC address of the VHT beamformee.

Source: IEEE Std 802.11-2016

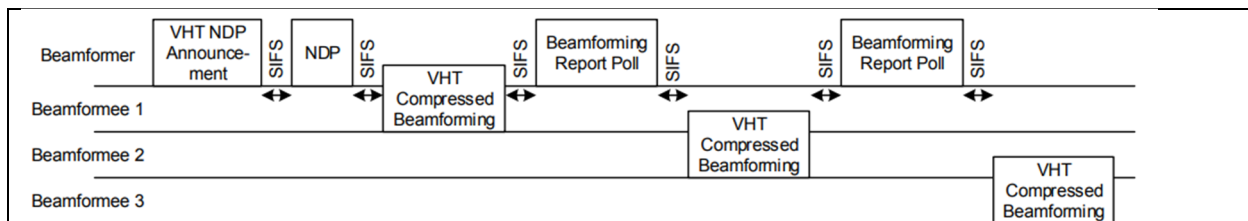


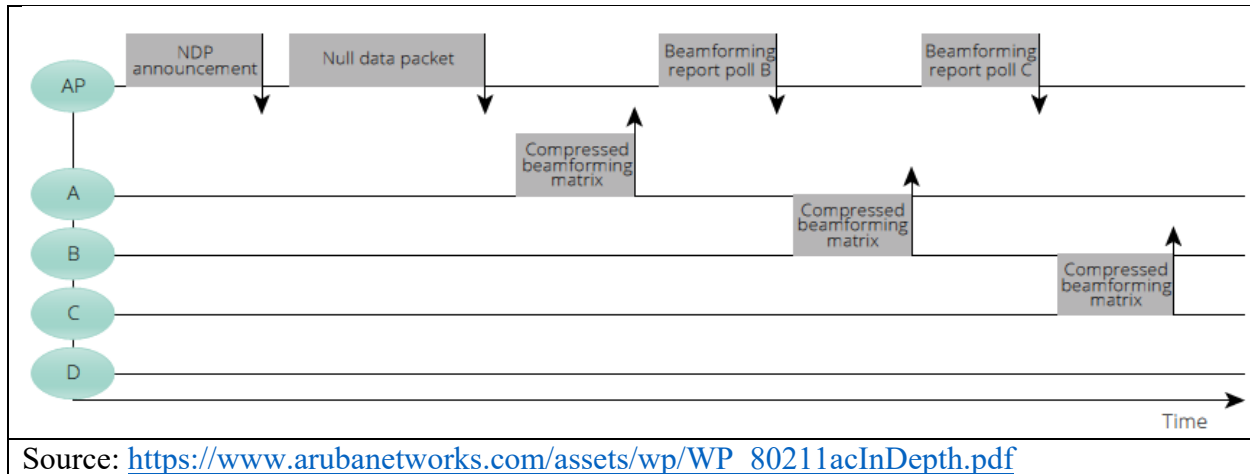
Figure 10-53—Example of the sounding protocol with more than one VHT beamformee

Source: IEEE Std 802.11-2016

First, the beamformer sends a null data packet announcement (NDPA) frame identifying the intended recipients and the format of the forthcoming sounding frame. This is followed by the sounding NDP itself, and the beamformee then responds with a beamforming report frame.

The NDPA and NDP frames are quite simple. The NDPA identifies which stations should listen to the subsequent sounding frame, along with the dimensions of that frame depending on the number of antennas and spatial streams in use. The sounding frame itself is just a null data packet: It is the preamble with its LTFs that is of importance. The processing and construction of the beamforming report, however, is complicated.

Source: https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf



97. The method practiced by the '122 Accused Products includes the transmit announcement indication indicating that a second communication frame will follow the first communication frame:

10.34.5.2 Rules for VHT sounding protocol sequences

If the VHT NDP Announcement frame includes more than one STA Info field, the RA of the VHT NDP Announcement frame shall be set to the broadcast address. If the VHT NDP Announcement frame includes a single STA Info field, the RA of the VHT NDP Announcement frame shall be set to the MAC address of the VHT beamformee.

A VHT NDP shall be transmitted only following a SIFS after a VHT NDP Announcement frame. A VHT NDP Announcement frame shall be followed by a VHT NDP after SIFS.

Source: IEEE Std 802.11-2016

9.2.4.1 Frame Control field**9.2.4.1.1 General**

The first three subfields of the Frame Control field are Protocol Version, Type, and Subtype. The remaining subfields of the Frame Control field depend on the setting of the Type and Subtype subfields.

9.2.4.1.3 Type and Subtype subfields

The Type subfield is 2 bits in length, and the Subtype subfield is 4 bits in length. The Type and Subtype subfields together identify the function of the frame. There are three frame types: control, data, and

Table 9-1—Valid type and subtype combinations

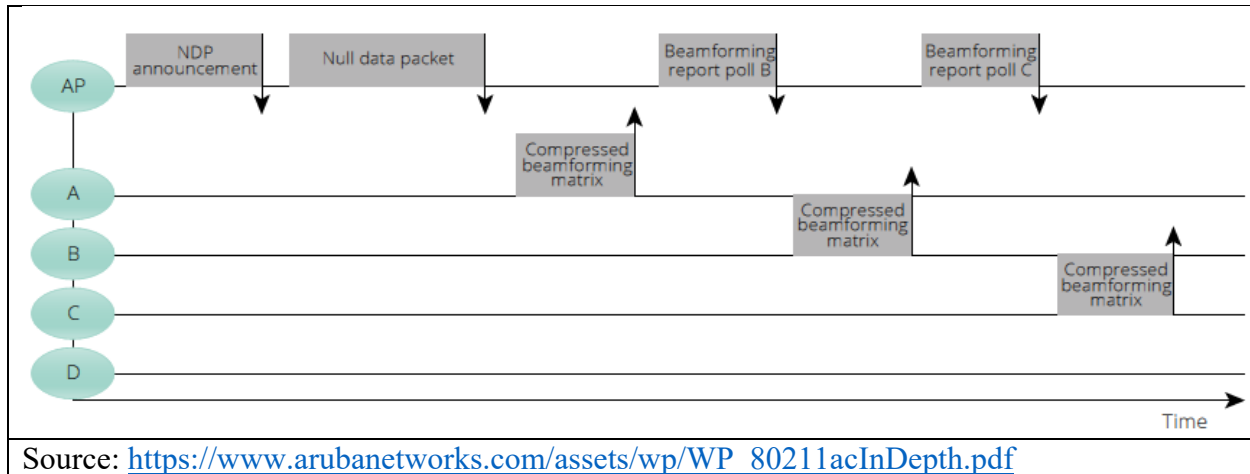
Type value B3 B2	Type description	Subtype value B7 B6 B5 B4	Subtype description
01	Control	0101	VHT NDP Announcement

Source: IEEE Std 802.11-2016

First, the beamformer sends a null data packet announcement (NDPA) frame identifying the intended recipients and the format of the forthcoming sounding frame. This is followed by the sounding NDP itself, and the beamformee then responds with a beamforming report frame.

The NDPA and NDP frames are quite simple. The NDPA identifies which stations should listen to the subsequent sounding frame, along with the dimensions of that frame depending on the number of antennas and spatial streams in use. The sounding frame itself is just a null data packet: It is the preamble with its LTFs that is of importance. The processing and construction of the beamforming report, however, is complicated.

Source: https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf



98. The method practiced by the '122 Accused Products includes a second communication frame intended for the second station will follow the first communication frame and that the second communication frame will not include the address of the second station:

10.34.6 Transmission of a VHT NDP

A VHT NDP shall use the SU PPDU format as described in 21.1.4. A STA shall transmit a VHT NDP using the following TXVECTOR parameters:

- APEP_LENGTH set to 0
- NUM_USERS set to 1
- NUM_STS indicates two or more space-time streams
- CH_BANDWIDTH set to the same value as the TXVECTOR parameter CH_BANDWIDTH in the preceding VHT NDP Announcement frame
- GROUP_ID and PARTIAL_AID are set as described in 10.20

Source: IEEE Std 802.11-2016

10.20 Group ID and partial AID in VHT PPDU

The partial AID is a nonunique STA identifier defined in Table 10-9. The partial AID is carried in the TXVECTOR parameter PARTIAL_AID of a VHT SU PPDU and is limited to 9 bits.

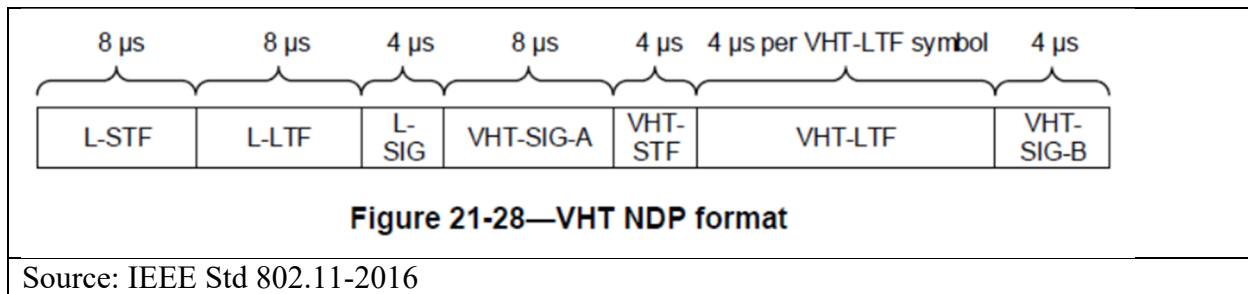
A STA transmitting a VHT SU PPDU carrying one or more group addressed MPDUs or transmitting a VHT NDP intended for multiple recipients shall set the TXVECTOR parameters GROUP_ID to 63 and PARTIAL_AID to 0. The intended recipient of a VHT NDP is defined in 10.34.6.

Source: IEEE Std 802.11-2016

10.34.5.2 Rules for VHT sounding protocol sequences

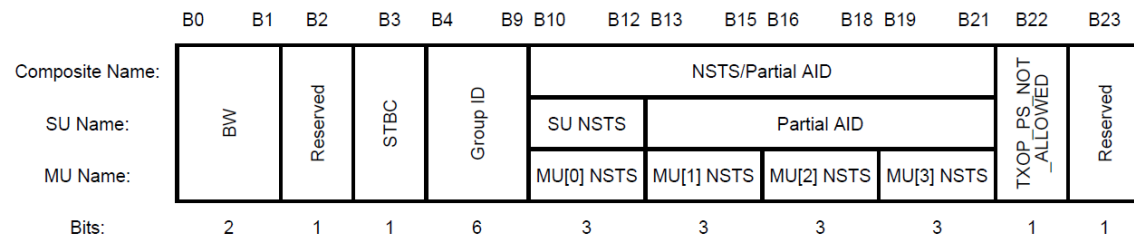
If the VHT NDP Announcement frame includes more than one STA Info field, the RA of the VHT NDP Announcement frame shall be set to the broadcast address. If the VHT NDP Announcement frame includes a single STA Info field, the RA of the VHT NDP Announcement frame shall be set to the MAC address of the VHT beamformee.

Source: IEEE Std 802.11-2016



21.3.8.3.3 VHT-SIG-A definition

The VHT-SIG-A field carries information required to interpret VHT PPDU. The structure of the VHT-SIG-A field for the first part (VHT-SIG-A1) is shown in Figure 21-18 and for the second part (VHT-SIG-A2) is shown in Figure 21-19.

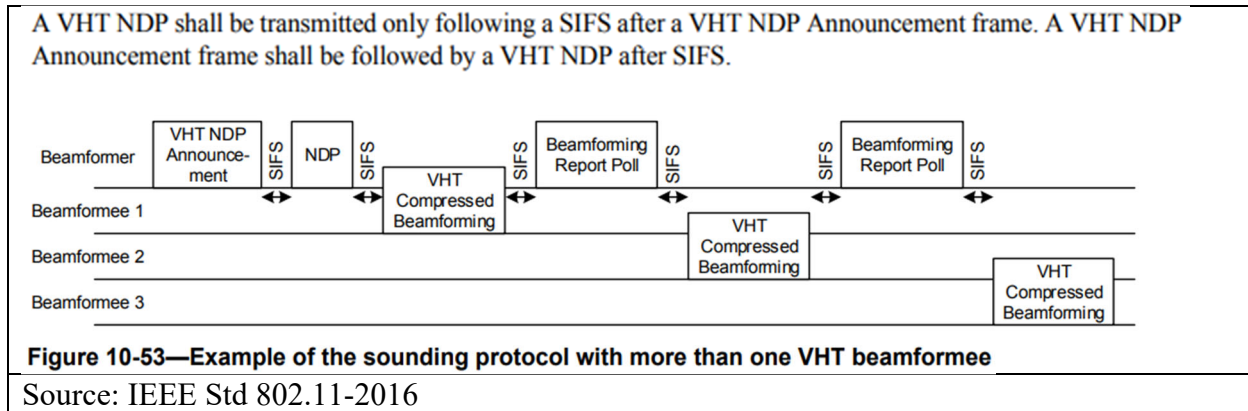


99. The method practiced by the '122 Accused Products includes the second communication frame follows after a short inter frame space (SIFS) after the first communication frame with the transmit announcement indication:

10.34.5.2 Rules for VHT sounding protocol sequences

A VHT beamformer shall initiate a sounding feedback sequence by transmitting a VHT NDP Announcement frame followed by a VHT NDP after a SIFS. The VHT beamformer shall include in the VHT NDP Announcement frame one STA Info field for each VHT beamformee that is expected to prepare VHT Compressed Beamforming feedback and shall identify the VHT beamformee by including the VHT beamformee's AID in the AID subfield of the STA Info field. The VHT NDP Announcement frame shall include at least one STA Info field.

Source: IEEE Std 802.11-2016



100. HPE has had knowledge of the '122 patent since at least as early as the receipt of IV's November 13, 2022 notice letter, which attached a copy of the '122 patent, and will receive further knowledge by service upon HPE of the Complaint in this Case.

101. Additionally, HPE has been, and currently is, an active inducer of infringement of the '122 patent under 35 U.S.C. § 271(b) and a contributory infringer of the '122 patent under 35 U.S.C. § 271(c).

102. HPE has actively induced, and continues to actively induce, infringement of the '122 patent by causing others to use, offer for sale, or sell products or services covered by the '122 patent, including the '122 Accused Products. HPE provides these products and services to others, such as customers, resellers, partners, and end-users, who, in turn, use, provision for use, offer for sale, or sell those products and services, which directly infringe the '122 patent. HPE's inducement includes the directions and instructions found at:

- <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/530-series/>
- <https://blogs.arubanetworks.com/solutions/11ac-beamforming-makes-the-dog-rollover/>
- https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf
- <https://community.arubanetworks.com/blogs/arunkumar1/2020/10/20/how-does-explicit-beamforming-work>

103. HPE has contributed to, and continues to contribute to, the infringement of the '122 patent by others by selling the '122 Accused Products, which, when installed, configured, and used directly infringe the '122 patent.

104. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe, and would actively induce and contribute to the infringement of, the '122 patent.

105. HPE has committed, and continues to commit, contributory infringement by selling products and services that directly infringe the '122 patent when used by a third party, such as the '122 Accused Products, and that are a material part of the invention, knowing them to be especially made or adapted for use in infringement of the '122 patent and not staple articles or commodities of commerce suitable for substantial non-infringing use.

106. As a result of HPE's acts of infringement, Intellectual Ventures I has suffered and will continue to suffer damages in an amount to be determined at trial.

PRAYER FOR RELIEF

Defendants request that the Court enter judgment:

- (A) that HPE has infringed the asserted counterclaim patents;
- (B) awarding damages sufficient to compensate defendants for HPE's infringement under 35 U.S.C. § 284;
- (C) finding this case exceptional under 35 U.S.C. § 285 and awarding defendants their reasonable attorneys' fees;
- (D) awarding its costs and expenses incurred in this action;
- (E) awarding prejudgment and post-judgment interest; and

(F) granting such further relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Defendants demand trial by jury of all claims so triable under Federal Rule of Civil

Procedure 38.

Dated: November 14, 2022

Respectfully submitted,

OF COUNSEL:

FARNAN LLP

Matthew D. Vella
mvella@princelobel.com
Robert R. Gilman
rgilman@princelobel.com
Jonathan DeBlois
jdeblois@princelobel.com
Aaron S. Jacobs
ajacobs@princelobel.com
PRINCE LOBEL TYE LLP
One International Place, suite 3700
Boston, MA 02110
Tel: 617-456-8000

/s/ Michael J. Farnan
Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market Street, 12th floor
Wilmington, DE 19801
Tel: 302-777-0300
Fax: 302-777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Attorneys for Defendants